Windows Server 2008系统工程师 视频突击



Windows Server 2008 安全内幕

刘晓辉　李利军　编著

超值赠送 DVD 20小时的Windows Server 2008安全管理视频操作

清华大学出版社

Windows Server 2008 系统工程师视频突击

Windows Server 2008 安全内幕

刘晓辉　李利军　编　著

清华大学出版社
北　京

内 容 简 介

本书全面阐述 Windows Server 2008 网络操作系统的安全配置和应用，主要内容包括 Windows Server 2008 系统基本安全措施、增强型安全配置、用户账户安全、活动目录安全、组策略安全、文件系统安全、高级防火墙、系统事件和性能监视、数字证书、VPN 连接、NAP、网络应用服务安全等多个方面。通过阅读本书，读者可以快速掌握 Windows Server 2008 系统安全基本配置内容，迅速成长为拥有专业技术的系统安全工程师。

本书可作为大专院校计算机相关专业的教材，也适合具有一定基础的系统管理员和网络管理员阅读。

图书在版编目(CIP)数据

Windows Server 2008 安全内幕/刘晓辉，李利军编著. —北京：清华大学出版社，2009.11
(Windows Server 2008 系统工程师视频突击)
ISBN 978-7-302-21138-9

Ⅰ. W…　Ⅱ. ①刘…　②李…　Ⅲ. 服务器—操作系统(软件)，Windows Server 2003—安全技术　Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字(2009)第 175764 号

责任编辑： 张　瑜
装帧设计： 杨玉兰
责任校对： 王　晖
责任印制：

出版发行： 清华大学出版社　　**地　址：** 北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：** 100084
社 总 机： 010-62770175　　**邮　购：** 010-62786544
投稿与读者服务： 010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈： 010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　销： 全国新华书店
开　本： 210×280　**印　张：** 36　**字　数：** 1027 千字
附 DVD 1 张
版　次： 2009 年 11 月第 1 版　**印　次：** 2009 年 11 月第 1 次印刷
印　数： 1~4000
定　价： 66.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：

前　　言

随着全球信息化程度的不断提高，计算机应用已经延伸到每个行业的各个领域，成为人们日常生活中不可或缺的一部分。根据某权威机构调查数据显示，截至 2008 年底，全球正在运行的计算机数量已经超过 10 亿台，中国占大半部分，在未来 5 年时间内，全球计算机数量将超过 20 亿台，并且中国增速会超过其他国家。中国不仅是计算机大国，而且是受病毒侵扰的大国，约有 20%的计算机被植入木马，并被恶意用户所劫持和控制。究其主要原因，大多是用户安全防范意识差所致。

许多人认为 Windows 操作系统是不安全的，其实并非如此。客观地讲，没有绝对安全的操作系统，任何操作系统的安全都是相对的。Linux 和 UNIX 也并非固若金汤，也同样会有系统漏洞，也同样会遭遇各种攻击。Windows Server 2008 已经度过了她一岁的生日，就现在的情况来看，无论安全性还是可靠性都得到了广大用户的认可。网络安全同样适用于 “木桶原理”，即网络安全涉及诸多方面，而最终导致问题出现的往往是安全性最差的那块“短板”。Windows 系统之所以往往充当“短板”角色，原因并不在于操作系统本身的安全架构和设计。即使操作系统本身已经很安全，但因为使用的人缺乏安全意识，也有可能导致操作系统在提高安全性方面所作的全部努力付之东流。

操作系统作为所有计算机资源的“统治者”，是一切应用程序的基础和核心。如果没有操作系统的安全，任何应用和管理都无从谈起。因此，操作系统的安全是整个计算机系统安全的基础。做事效率高当然是件好事，但是如果本末倒置，一切都将归零。不对初装的服务器系统进行安全设置就投入使用，无异于开发商没拿到批文就开工，司机没有取得驾驶证就开车上路，最终结局只有一个——自食恶果。其实，许多安全入侵事件都是由网络管理员或用户的疏忽或疏漏所导致，如果合理配置、全面扫描、完善各种审核机制，完全可以避免大多数的攻击。

相对于 Windows Server 2003，Windows Server 2008 的最大改进就是系统安全性的提升。在继承和发展了原有安全架构的基础上，新推出的 NAP(网络访问限制)技术极大地提高了网络客户接入的安全性，RFM(综合权限管理)可以有效地保护敏感数据的安全，只读域控制器提高了活动目录的安全性，增强型 VPN 连接则能确保用户远程访问的私密性。

全书以系统安全配置为中心，配合大量的操作演示，从多个角度揭开 Windows Server 2008 系统安全的神秘面纱。本书共分为 15 章，主要内容涵盖 Windows Server 2008 系统基本安全措施、增强型安全配置、活动目录安全、防火墙、NAP 等多个方面。其中，重点的网络应用安全，如活动目录、文件服务器、NAP 的内容在本书的篇幅上也有所体现。

本书由刘晓辉、李利军编著，田俊乐、李海宁、赵卫东、刘淑梅、马倩、杨伏龙、李文俊、王同明、石长征、莫展宏、白华、郭腾、王淑江、王春海、陈志成、刘国增、王延杰及刘红等也参与了部分章节的编写工作。作者长期从事网络的搭建、配置和管理工作，具有丰富的网络管理实践经验，曾经出版过多部计算机类图书，均以易读、易学且实用的特点受到众多读者的一致好评。本书是作者的又一呕心沥血之作，希望对大家的操作系统安全配置与维护工作能有所帮助。

编　者

目　　录

第 1 章　Windows Server 2008 初始安全

Windows Server 2008 是 Microsoft 公司的扛鼎之作，是目前功能最强大的网络服务器操作系统，不仅系统和网络功能有了一定的扩展，更重要的是安全性也有了很大提高。Windows Update、Windows 防火墙、安全配置向导、防间谍软件等功能，可以帮助用户做好基本的安全防护工作。若想完全利用这些功能，打造无懈可击的服务器操作系统，就必须详细了解这些功能，并根据需要进行相应的设置。

关键词

- Windows Server 2008 安装安全
- Windows Server 2008 基本安全
- Windows Server 2008 被动防御安全
- Windows Server 2008 系统安全

1.1 Windows Server 2008 安装安全

安装操作系统是一切应用和配置的基础。安装方式的正确与否将直接影响后续安全工作的开展，因此实施安装之前应详细了解 Windows Server 2008 安装注意事项。如果是升级安装方式，还应及时下载补丁更新，以免导致升级安装的失败，或者升级完成后带来的安全隐患。

1.1.1 系统安装安全指南

安装 Windows Server 2008 时应注意以下几点：

- 使用正版 Windows Server 2008 系统安装光盘，防止安装过程中被植入木马或间谍软件，影响系统安全性。另外，盗版系统安装光盘也可能影响计算机的兼容性，导致一些莫名其妙的问题。
- 保证硬件设备的可靠性。建议为重要服务器使用磁盘阵列冗余技术，如 RAID 5 等，确保服务器存储系统硬件的稳定性和安全性。
- 尽量使用全新方式安装系统，即将操作系统安装在一个干净的系统分区中，并提前做好合理规划，避免安装完成后重新修改系统配置带来的麻烦。例如，安装之前删除系统分区的所有文件，并重新格式化，确保磁盘完好无损。
- 使用 NTFS 文件系统格式化服务器所有磁盘分区，可以为系统分区、数据分区和日志文件分区提供更高的安全性。NTFS 是真正的日志性文件系统，使用日志和检查点信息，即使在系统崩溃或者电源故障的时候也可以保证文件系统的一致性。只有使用 NTFS 格式的分区才能为文件提供访问权限控制，达到访问控制安全的目的。
- 没有进行任何安全配置的初装服务器不要与任何公共设备或网络连接，必要时可以找一台可以确保安全性的服务器进行连接。
- 只为服务器安装必需的协议，如 TCP/IP 协议，避免其他网络协议给系统带来的漏洞。
- 通常情况下，不要将服务器加入到域，而安装成独立服务器模式。
- 为系统管理员设置一个安全性较高的密码。
- 不要在服务器上部署多操作系统，防止恶意用户通过其他系统控制权限获取重要信息，或对 Windows Server 2008 系统进行破坏。
- 如果条件允许，建议安装英文版 Windows Server 2008。通常情况下，微软公司总是最先发布英文版本的补丁，中文版本的补丁相对滞后一段时间。

1.1.2 安全补丁更新

安全补丁更新是 Windows 系统必不可少的安全配置。默认情况下，Windows Server 2008 安装完成后，自动更新功能是未配置的，管理员必须开启并指定选择相应的方式，为系统下载、安装补丁更新，以保护系统的安全。主要配置步骤如下。

① 为 Windows Server 2008 配置系统更新之前，每次启动计算机后都会在任务栏的右侧系统托盘中，显示如图 1-1 所示的提示信息。

② 单击此提示信息打开如图 1-2 所示的 Windows Update 对话框。除此之外，在“初始配置任务”

窗口的“更新此服务器”选项区域，以及在“服务器管理器”窗口的“安全信息”选项区域中，同样可以启动 Windows Update 配置向导。

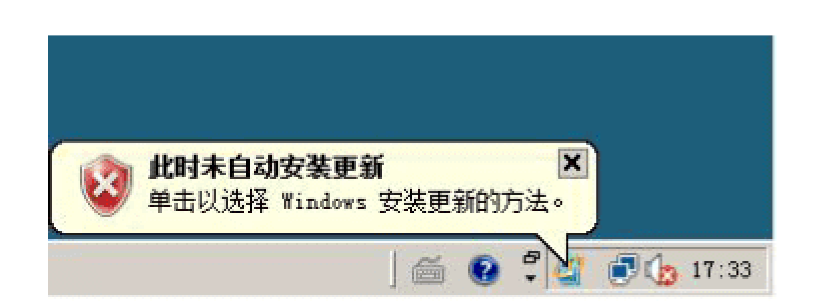


图 1-1　“此时未自动安装更新”提示

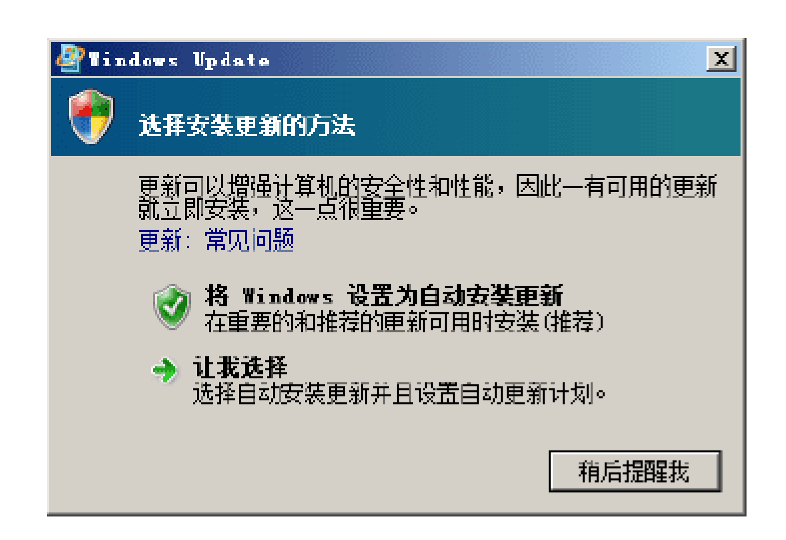


图 1-2　Windows Update 对话框



提示：只有第一次配置自动更新时才会显示该对话框，以后将不再显示。如果要让 Windows 系统自动下载并安装更新，可直接单击“将 Windows 设置为自动安装更新”，完成系统更新配置。

③　单击“让我选择”，打开如图 1-3 所示的“更改设置”对话框。在“选择 Windows 安装更新的方法”中，选择一种安装方法即可，各种安装方式的具体含义如下。

- 自动安装更新(推荐)：服务器连接到 Internet 后，系统将自动检测 Microsoft Update 服务器是否有所需更新，如果有则将自动下载并安装这些更新。选择该单选按钮后还需要指定系统自动安装更新的具体时间。
- 下载更新，但是让我选择是否安装更新：仅下载所需的系统更新，完成后通知用户在合适的时间手动安装。
- 检查更新，但是让我选择是否下载和安装更新：仅检测 Microsoft Update 服务器上提供的更新项目，并以列表方式提示系统管理员，管理员可以根据实际情况选择需要下载的系统更新。建议使用这种方式，可以减少不必要的服务器资源和网络带宽浪费。
- 从不检查更新(不推荐)：关闭系统更新功能，建议不要选择此项。



图 1-3　“更改设置”对话框

1.2 Windows Server 2008 基本安全

Windows Server 2008 基本安全配置包括 Internet 防火墙和安全配置向导。为确保 Windows Server 2008 服务器的安全，安装完成之后应立即启用并配置 Internet 防火墙，以便防止黑客或恶意软件通过网络或 Internet 访问计算机。安装网络服务之后，可以通过安全配置向导有针对性地部署网络访问安全策略。

1.2.1 Internet 连接防火墙

Internet 连接防火墙(Internet Connection Firewall，ICF)是 Windows 系统的内置防火墙，不仅可以阻止来自外部网络的恶意访问或攻击，还可以阻止当前服务器向其他计算机发送恶意软件。默认情况下，ICF 是自动开启的。

1. 防火墙简介

Windows Server 2008 的 ICF 是一种典型的状态防火墙，不仅可以监视通过其路径的所有通信，并且检查所处理的每一条消息的源地址和目的地址，工作方式如图 1-4 所示。

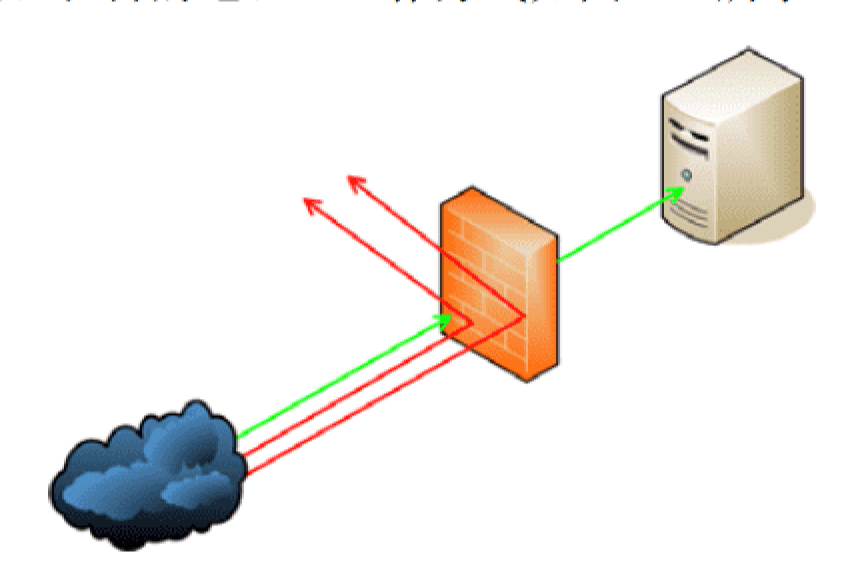


图 1-4 Internet 防火墙的工作方式

ICF 就像一个在计算机和外部 Internet 之间建立的“盾牌”，可以允许请求的数据包通过，而阻碍那些没有请求的数据包，因此它是一个动态数据包过滤器。它可以对直接连接 Internet 或连接在运行 ICF 的“Internet 连接共享主机”后的计算机提供保护。启用后，ICF 会禁止所有来自 Internet 的未经允许的连接。为此，防火墙使用“网络地址转换器(NAT)”逻辑来验证访问网络或本地主机的入站请求。如果网络通信不是来自受保护的网络内部，或者没有创建任何端口映射，入站数据就被丢弃。

通常情况下，黑客入侵的第一步就是找到所要攻击主机的 IP 地址，再使用 ping 命令 ping 通该主机(表示已经与该主机建立了一个通道)，然后对主机进行端口扫描，察看哪些端口是开放的，最后找出系统漏洞进行攻击。如果攻击个人电脑，通常是通过扫描一段 IP 地址开始来锁定目标，这种情况下，ping 不通的 IP 地址通常被认为没有使用而忽略过去。因此，ICF 的第一个功能就是不响应 ping 命令，而且，ICF 还禁止外部程序对本机进行端口扫描，抛弃所有没有请求的 IP 数据包。如此一来，可以被黑客利用的系统漏洞就很少了。

ICF 是通过保存一个表格，记录所有自本机发出的目的 IP 地址、端口、服务以及其他一些数据来达到保护本机的目的。当一个 IP 数据包进入本机时，ICF 会检查这个表格，看到达的这个 IP 数据包是不是本机所请求的，如果是就让它通过，如果在这个表格中没有找到相应的记录就抛弃这个 IP 数据包。

2. 配置 Internet 防火墙

Windows Server 2008 系统的 ICF 默认情况下已经启动，管理员可以根据需要进行配置。如果服务器已经连接到网络，则网络访问策略的设置可能会阻止管理员对 Windows 防火墙的配置。

① 在 Windows Server 2008 的“控制面板”窗口中，双击“Windows 防火墙”图标，显示如图 1-5 所示的窗口。本例中的 Windows 防火墙已启用。



图 1-5 “Windows 防火墙”窗口

② 单击“启用或关闭 Windows 防火墙”链接，打开如图 1-6 所示的“Windows 防火墙设置”对话框，系统默认选择“启用”单选按钮。如果同时选中“阻止所有传入连接”复选框，则防火墙将阻止所有主动连接当前服务器的尝试，除非需要为该服务器提供最大程度的保护时，才使用该设置，启用该设置后将忽略“例外”列表中的所有设置。通常情况下，不推荐选择该复选框。

③ 单击“例外”或者在“Windows 防火墙”窗口中单击“允许程序通过 Windows 防火墙”链接，则显示如图 1-7 所示的“例外”选项卡，在“程序或端口”列表框选中该服务器欲提供的网络服务即可。

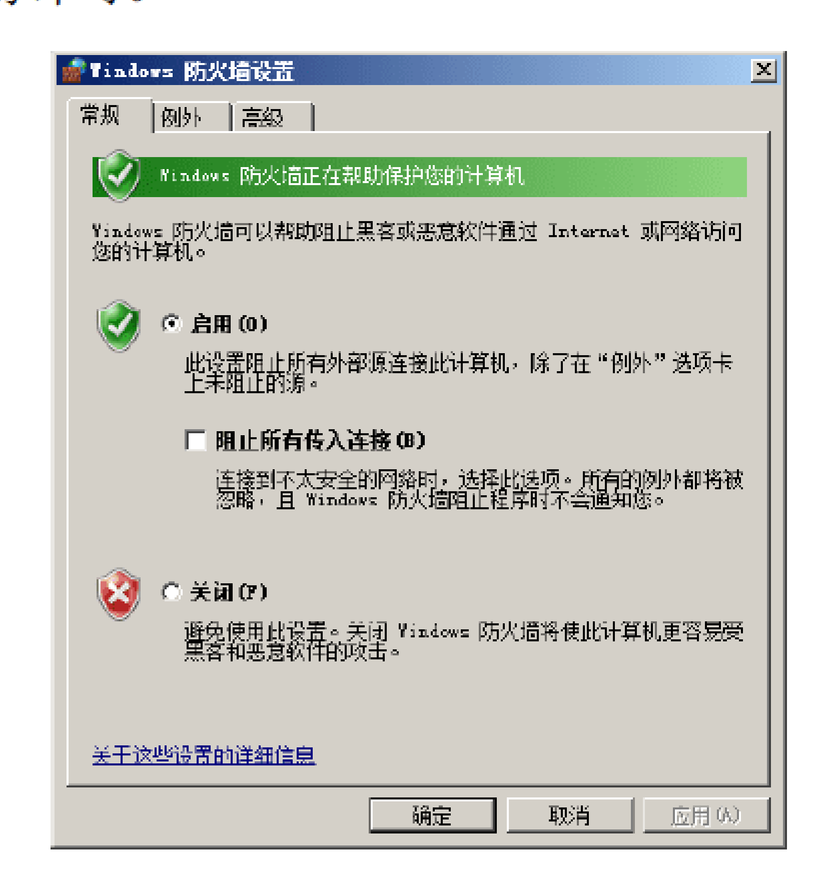


图 1-6 “Windows 防火墙设置”对话框



图 1-7 “例外”选项卡



提示：在“高级安全 Windows 防火墙”工具中，也可以查看 Windows 防火墙的“例外”设置。

④ 单击“添加端口”按钮，打开如图 1-8 所示的“添加端口”对话框，即可向列表中增加新的网络服务所使用的 TCP 或 UDP 端口。在“名称”文本框中输入便于识别的名称，如 telnet；在“端口号”文本框中输入想要添加的端口，如 23；根据需要选择 TCP 或 UDP 端口类型。

⑤ 单击“更改范围”按钮，打开如图 1-9 所示的“更改范围”对话框。指定详细的限定范围可以提高防火墙策略的安全性。默认情况下，开放的防火墙端口适用于任何计算机(包括 Internet 上的计算机)。

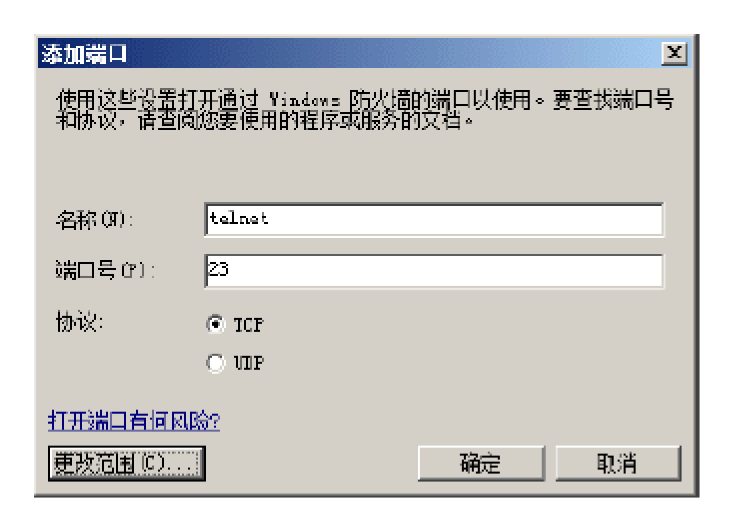


图 1-8 “添加端口”对话框



图 1-9 “更改范围”对话框



提示：选择“仅我的网络”单选按钮，则开放端口仅适用于本地计算机所在子网，对其他用户仍然关闭。选择“自定义列表”单选按钮，则可以根据需要指定详细的 IP 地址或子网范围。

⑥ 单击“高级”标签，切换至如图 1-10 所示的“高级”选项卡，在“网络连接设置”选项区域，可以设置接受 Windows 防火墙保护的网络连接，默认为所有本地连接。在“默认设置”选项区域，单击“还原为默认值”按钮即可撤销所有 Windows 防火墙设置，恢复至初始状态。需要注意的是，必须是本地计算机上 Administrators 组的成员，或者是被委派了适当的权限的用户，才可以还原 Windows 防火墙默认设置。如果计算机已经加入到某个域中，则 DomainAdmins 组的成员可以执行该过程。

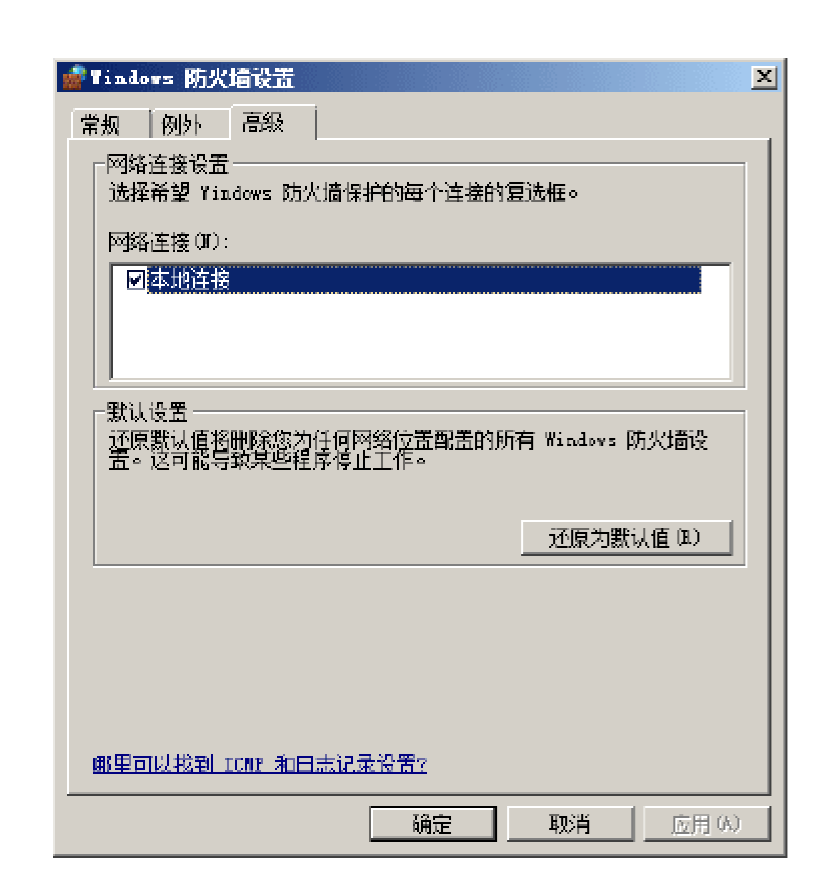


图 1-10 “高级”选项卡



提示： 与 Windows Server 2003 的 Internet 防火墙不同的是，“高级”选项卡中的“ICMP”相关设置已被转移到“高级安全 Windows 防火墙”中。

⑦ 单击“确定”按钮，保存设置即可。

1.2.2 安全配置向导

安全配置向导(SCW)可以帮助管理员快速完成创建、编辑、应用和回滚安全策略操作。用户可以根据需要创建针对某个服务器角色的安全策略，并且可以将其应用到其他服务器上。配置和应用 SCW 时应注意以下几点：

- SCW 禁用不需要的服务并提供对具有高级安全性的 Windows 防火墙的支持。
- 使用 SCW 创建的安全策略与安全模板不同，其中前者扩展名为.xml，而后者扩展名为.inf。用户创建的安全策略源于安全模板，安全模板包含的安全设置可以应用于所有的服务器角色。
- 部署 SCW 安全策略后并不会影响服务器提供服务时所需的组件，并且应用之后，管理员仍可以通过服务器管理器安装所需的组件。
- 应用 SCW 安全策略之后，SCW 将自动选择所有从属角色。
- 创建和应用 SCW 安全策略时，应确保服务器的 IP 协议及端口配置完全正确。

1. 创建安全策略

① 依次单击“开始”→“管理工具”→“安全配置向导”命令，打开如图 1-11 所示的“欢迎使用安全配置向导”界面。也可以在“开始”菜单的“开始搜索”文本框中输入 SCW 命令，单击“确定”按钮来启动安全配置向导。

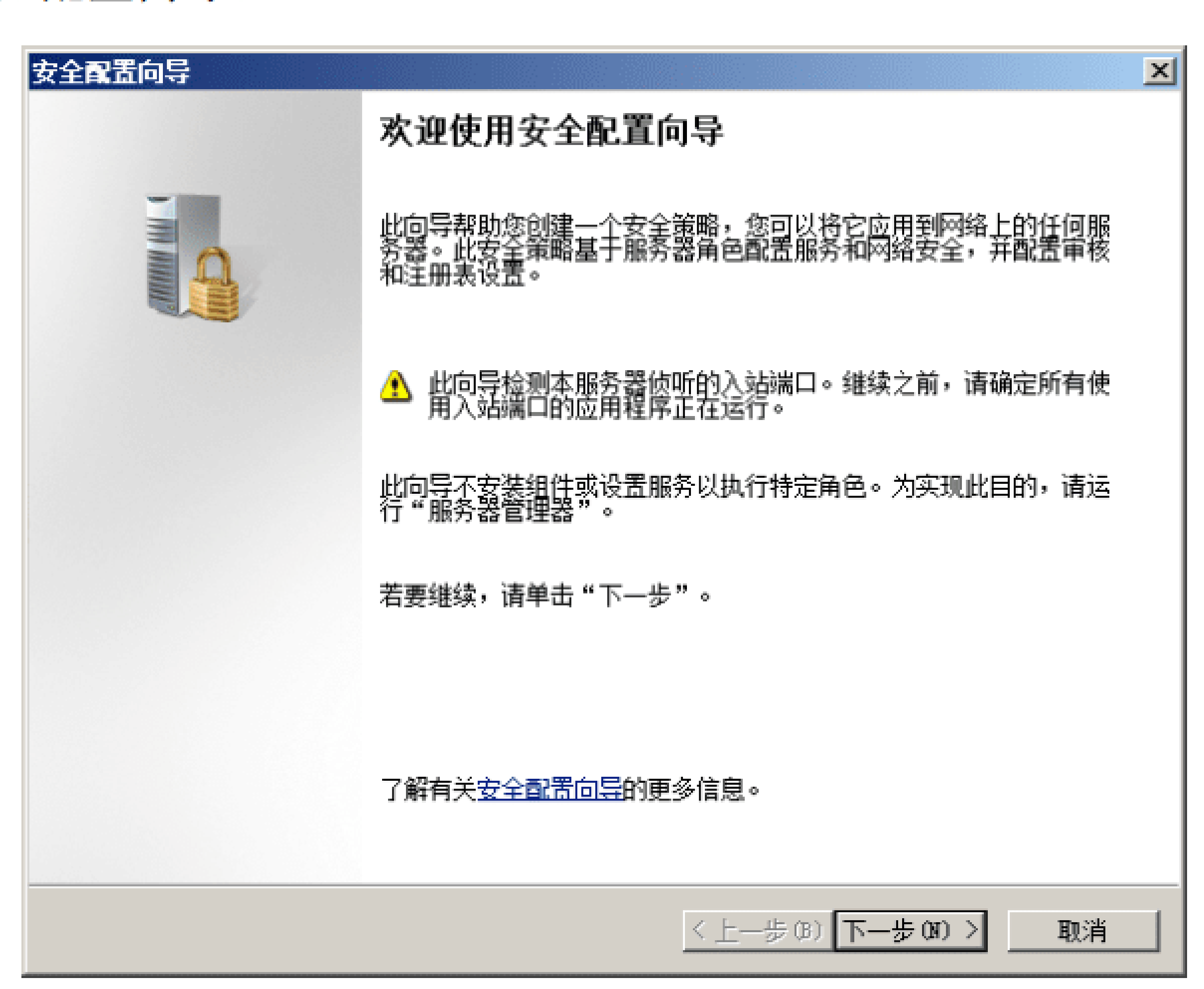


图 1-11 “欢迎使用安全配置向导”界面

② 单击“下一步”按钮，显示如图 1-12 所示的“配置操作”界面。

安全配置向导提供了 4 种配置操作。

- 新建安全策略：可以创建用于配置服务、Windows 防火墙、Internet 协议安全(IPSec)设置、审核

策略和特定注册表设置的安全策略。安全策略文件是 XML 格式文件，默认保存路径为%systemroot%\security\msscw\Policies。

- 编辑现有安全策略：可以编辑已使用 SCW 创建的安全策略。必须先选择“编辑现有安全策略”，才能浏览到要编辑的安全策略文件所在的文件夹。编辑的策略可存储在本地或网络共享文件夹中。
- 应用现有安全策略：使用 SCW 创建安全策略后，可将其应用到测试服务器，或者应用到生产环境。



提示：在将新创建或新修改的安全策略应用到生产环境之前，首先进行测试，然后将安全策略部署到业务系统中，测试可使新策略在生产环境中导致意外结果的可能性降至最低。

- 回滚上一次应用的安全策略：如果使用 SCW 应用的安全策略使服务器功能达不到预期的效果，或者导致其他非预期结果，则可以回滚该安全策略，将自动从该服务器删除对应的安全策略。

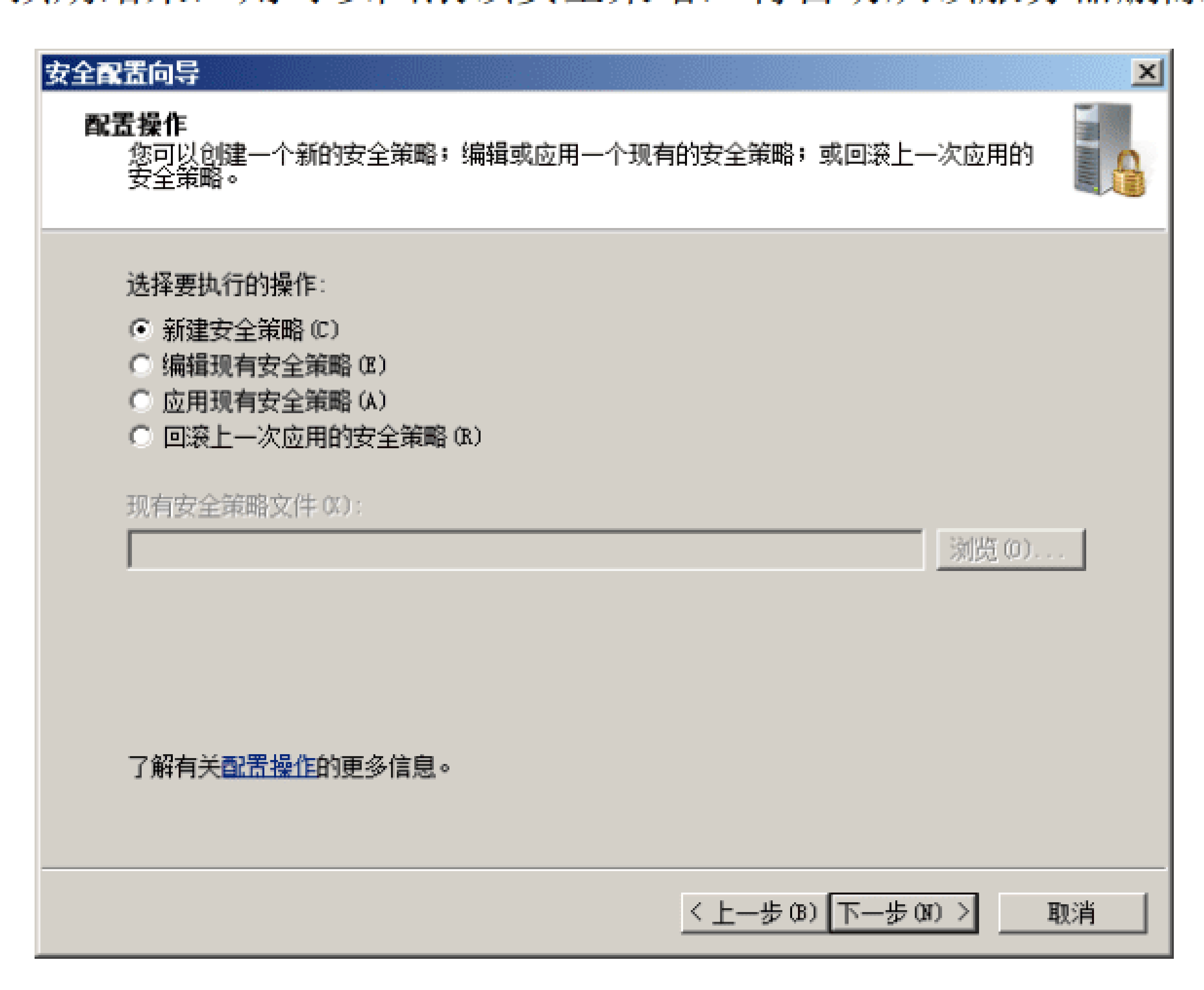


图 1-12 “配置操作”界面



注意：如果策略是在“本地安全策略”中编辑的，在应用策略后，这些更改就不能回滚到应用前的状态。对于服务和注册表值，回滚过程还原了在配置过程中更改的设置。对于 Windows 防火墙和 IPsec，回滚过程取消当前使用的任何 SCW 策略的分配，并重新分配在配置时使用的前策略。

如果是第一次使用安全配置向导，则应选择“新建安全策略”单选按钮。

③ 单击“下一步”按钮，显示如图 1-13 所示的“选择服务器”界面。在“服务器”文本框中，输入需要进行安全配置的 Windows Server 2008 服务器的主机名或 IP 地址。也可以单击“浏览”按钮，选择需要进行安全配置的目标计算机。

④ 单击“下一步”按钮，开始扫描配置数据库，主要包括已安装或运行的网络服务、IP 地址及子网信息等。扫描完成后显示“正在处理安全配置数据库”界面。单击“查看配置数据库”按钮，可以查看详细扫描结果。需要注意的是，在此过程中由于 Internet Explorer 7.0 的安全设置，可能会出现安全提示信息。单击“下一步”按钮，显示“基于角色的服务配置”界面，如图 1-14 所示。

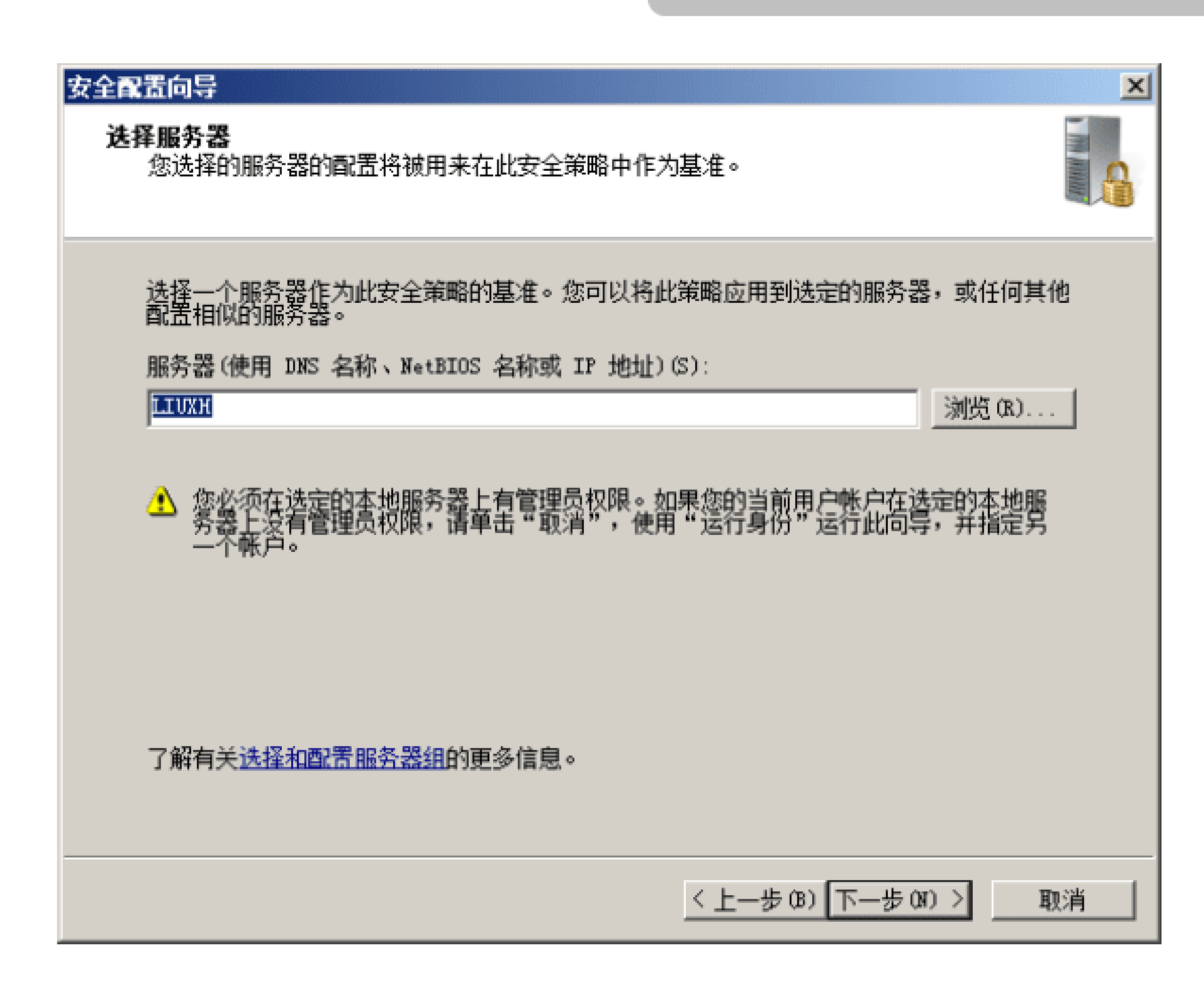


图 1-13 “选择服务器”界面

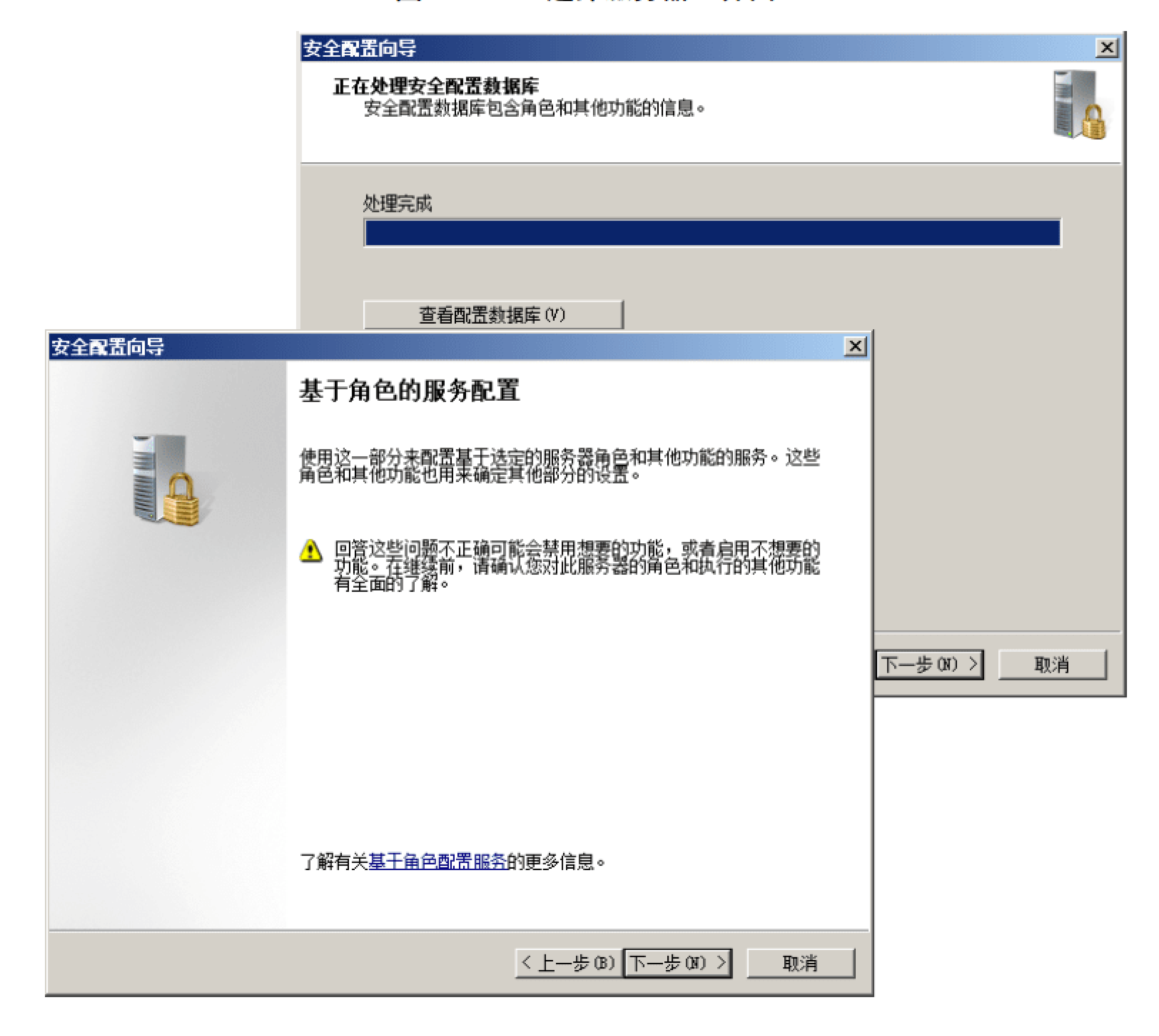


图 1-14 “正在处理安全配置数据库”和“基于角色的服务配置”界面

⑤ 单击“下一步”按钮，显示如图 1-15 所示的“选择服务器角色”界面。系统默认选择“安装的角色”选项，即只设置已安装服务的安全策略。“查看”下拉列表框中提供了 4 种可供选择的抉择模式。

- 所有角色：列出所有的 Windows Server 2008 可以使用的角色。
- 安装的角色：列出当前服务器中已经安装的角色，包括没有设置的角色。
- 未安装的角色：列出当前服务器中没有安装的角色，不包括没有设置的角色。

■ 选定的角色：列出当前服务器中已经选定的角色。



图 1-15 “选择服务器角色”界面

> **注意：** 为了保证服务器的安全，仅选择所需要的服务器角色即可，如本例中选择“Web 服务器”。选择多余的服务器角色，会增加 Windows Server 2008 系统的安全隐患。

⑥ 单击“下一步”按钮，显示如图 1-16 所示的“选择客户端功能”界面，可以选择当前服务器作为其他服务器的客户端时需要使用的功能，如自动更新客户端等。“查看”下拉列表中的选项与“选择服务器角色”中的完全相同，此处不再赘述。

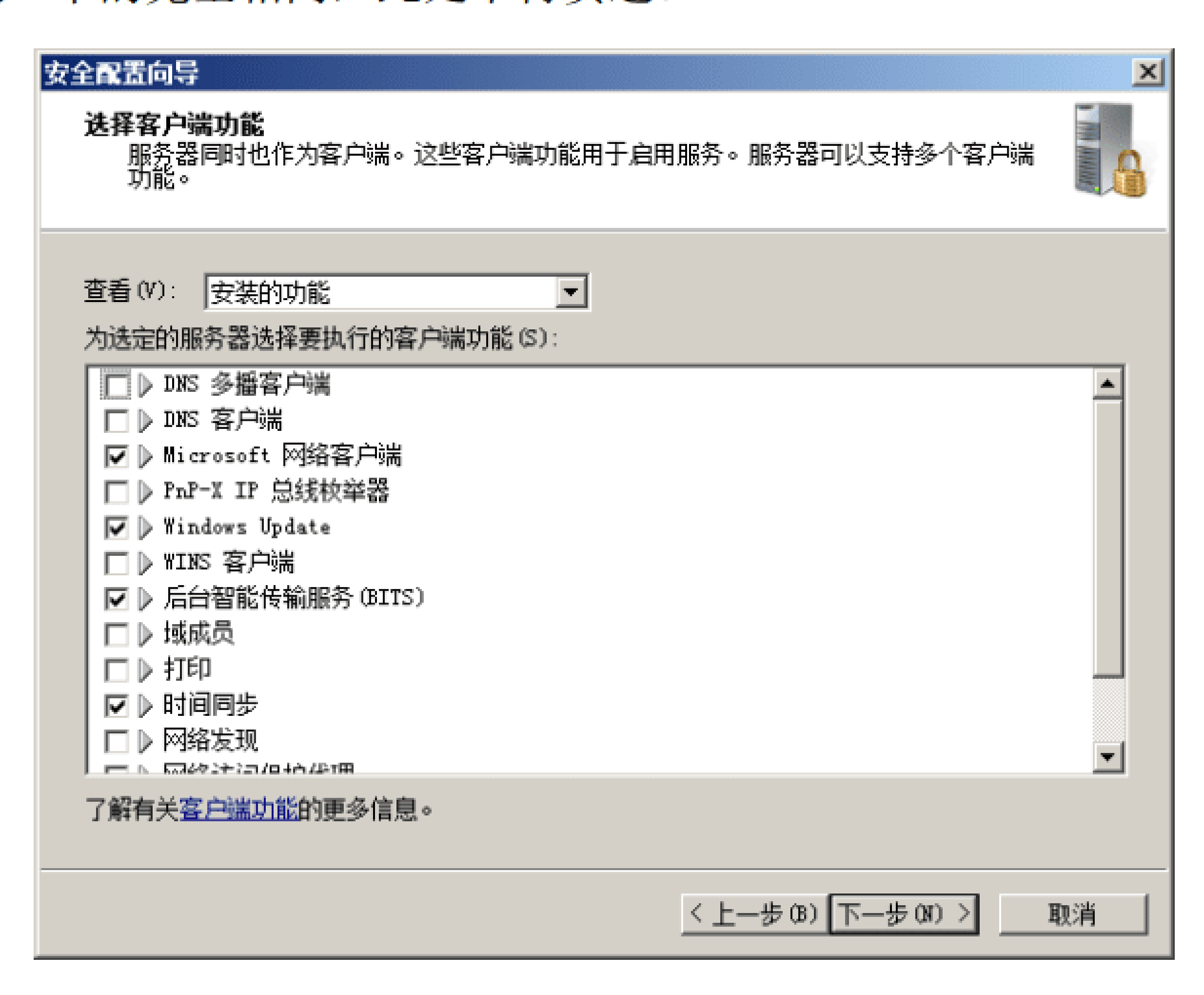


图 1-16 “选择客户端功能”界面

⑦ 单击“下一步”按钮，显示如图 1-17 所示的“选择管理和其他选项”界面。在“选择用来管理选定的服务器的选项”列表中，可以选择相应的管理选项。

⑧ 单击“下一步”按钮，显示“选择其他服务”界面。其他服务是指当前服务器上已经安装但在安

全配置数据库中未显示的服务。如果出现这种情况，安全配置向导将在“选择其他服务”界面上显示已安装的服务列表。展开相应的服务即可查看其详细运行模式，如图 1-18 所示。



图 1-17　“选择管理和其他选项”界面

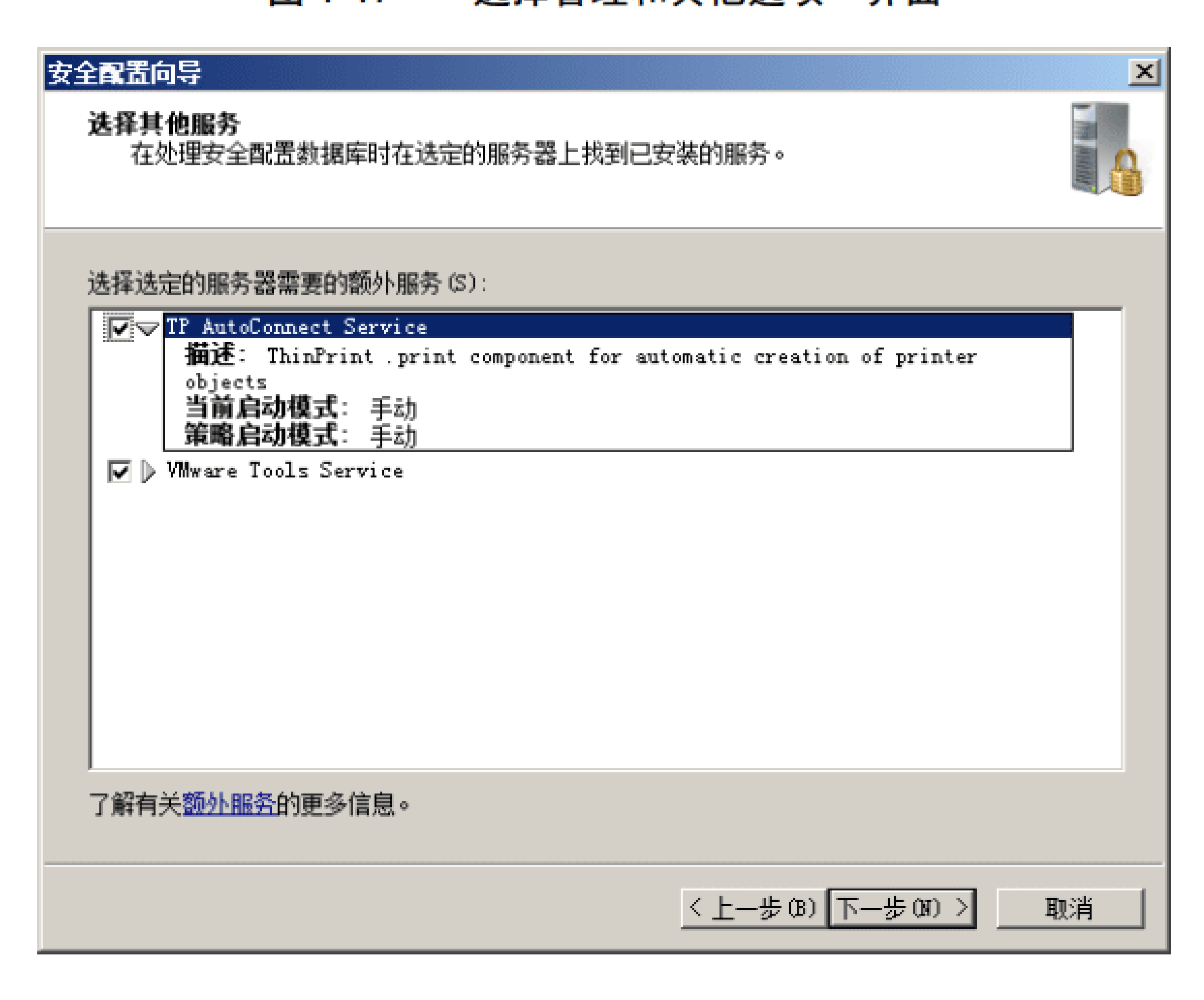


图 1-18　“选择其他服务”界面

⑨ 单击“下一步”按钮，显示如图 1-19 所示的“处理未指定的服务”界面。“未指定服务”是指安全策略配置向导扫描过程中未能发现的服务，用户可以在这里设置其运行状态，选择“不更改此服务的启动模式”单选按钮即可。

两者处理方式的主要区别如下。

- 保持服务的当前启动模式：如果选择此选项，则在应用此安全策略的服务器上启用的未指定服务将保持启用状态，而禁用的那些服务将保持禁用状态。
- 禁用服务：如果选择此选项，则不在安全配置数据库中的或未安装在选定服务器上的所有服务都将被禁用。



图 1-19 “处理未指定的服务”界面

⑩ 单击“下一步”按钮，显示如图 1-20 所示的“确认服务更改”界面，系统默认只显示当前服务器上正在运行的服务，服务的启动模式可以是“已禁用”、“手动”或“自动”。在应用安全策略后，才能对选定服务器做出更改。



图 1-20 “确认服务更改”界面

⑪ 单击“下一步”按钮，显示“网络安全”界面。如果选中“跳过这一部分”复选框，则将跳过“网络安全”配置部分。建议不要跳过此步骤，继续按照如下步骤操作。单击“下一步”按钮，显示“网络安全规则”界面。系统默认显示“所有规则”，即该服务器上目前开放的所有端口。也可以在“查看”下拉列表中选择其他查看方式。单击安全规则前面的三角形按钮，还可以查看其详细信息，如图 1-21 所示。



图 1-21　“网络安全”和“网络安全规则”界面



提示：如果列表中没有列出需要使用的 Windows 防火墙规则，可以单击“添加”按钮，打开如图 1-22 所示的“添加规则”对话框，将其添加到列表中。在“名称”文本框中，输入防火墙规则的名称，如 www，为了便于区分，还可以输入相关的描述信息；在“方向”选项组中，选择“入站”单选按钮；另外，还可以根据需要在“操作”选项组中选择相应的限制连接方式。

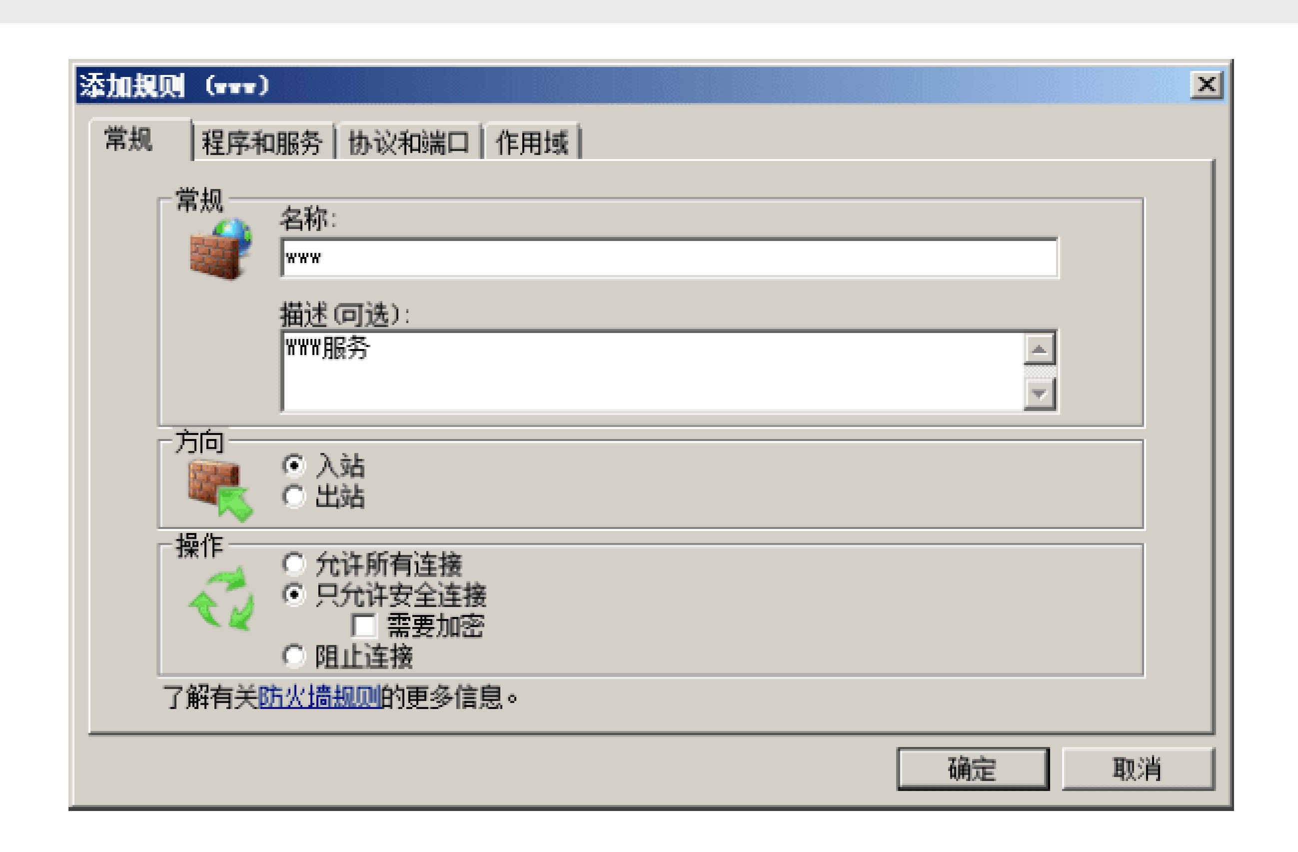


图 1-22　“添加规则”对话框

⑫　单击“下一步”按钮，显示“注册表设置”界面。通过该设置可以修改 Windows Server 2008 服务器注册表中的一些特殊键值，从而严格限制用户的访问权限。建议用户不要跳过此步骤。单击“下一步”按钮，显示“要求 SMB 安全签名”界面。设置选定的服务器和客户端的通信信息，保持系统默认的全部选择状态即可，如图 1-23 所示。



图 1-23 “注册表设置”和“要求 SMB 安全签名”界面

⑬ 单击“下一步”按钮，显示如图 1-24 所示的“出站身份验证方法”界面。选择当前服务器远程连接到其他计算机时使用的身份验证方法，如果是在域网络中进行远程登录，则选中“域账户”复选框即可；如果是工作组环境，建议选中“远程计算机上的本地账户”复选框。

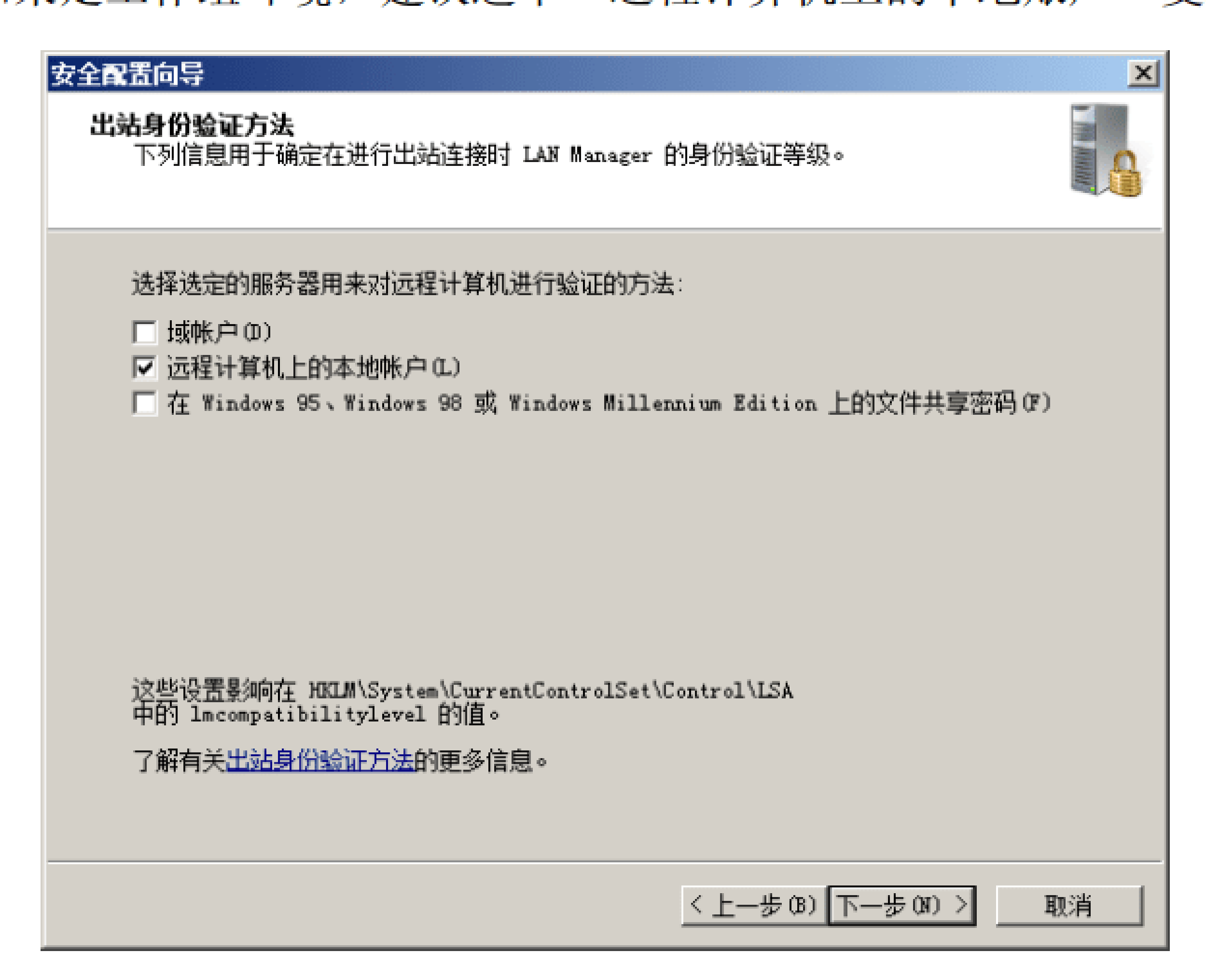


图 1-24 “出站身份验证方法”界面

⑭ 单击“下一步”按钮，显示如图 1-25 所示的“出站身份验证使用本地账户”界面，此界面中的选项与所选择的出站身份验证方法有关，这里以使用“远程计算机上的本地账户”验证方法为例。通常情况下，保持默认设置即可。

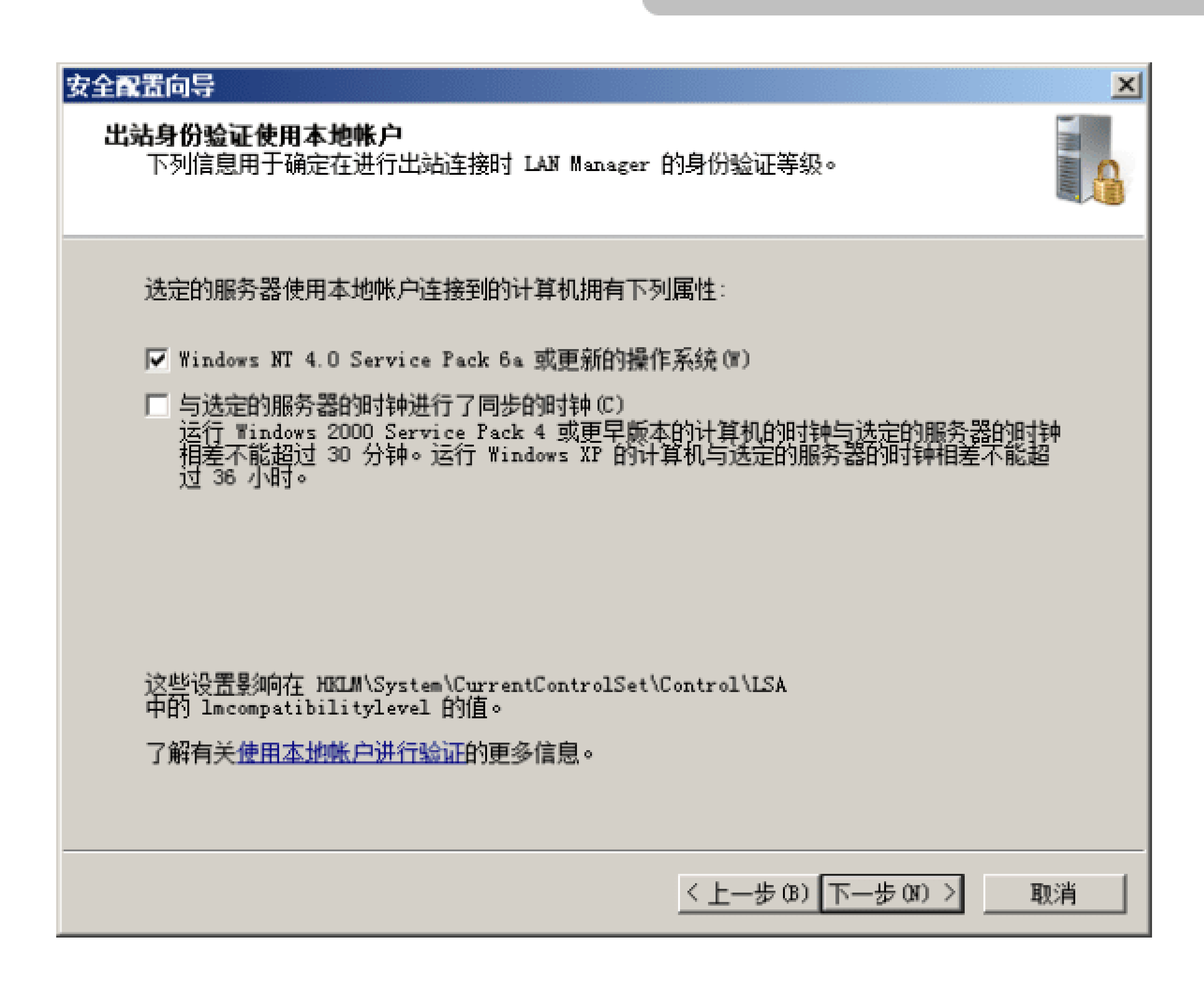


图 1-25　“出站身份验证使用本地账户”界面



提示： 如果不选择任何出站身份验证方法，则单击“下一步”按钮将提示设置入站设置选项，如图 1-26 所示。入站身份验证方法主要用于确定当网络用户访问当前计算机时需要使用哪种身份验证方法。如果设置了“出站身份验证方法”则不会出现该对话框。



图 1-26　“入站身份验证方法”界面

⑮ 单击“下一步”按钮，显示如图 1-27 所示的“注册表设置摘要”界面，显示了当前安全策略中所做的注册表安全设置。

⑯ 单击“下一步”按钮，显示“审核策略”界面。Windows 审核策略主要用于审核日志记录中的相关内容，并确定受影响的系统对象。安全策略回滚功能是无法回滚安全向导中的审核策略设置的。单击“下一步”按钮，显示“系统审核策略”界面。选择需要审核的目标，选择“审核成功的操作”单选按钮，即只审核日志记录中操作成功的事件记录，如图 1-28 所示。

⑰ 单击“下一步”按钮，显示如图 1-29 所示的“审核策略摘要”界面。列表中列出了应用策略时，

将在选定服务器上对审核策略进行的所有更改。此界面显示每个审核策略设置的当前设置和由策略定义的设置。



图 1-27 “注册表设置摘要”界面



图 1-28 “审核策略”和“系统审核策略”界面

⑱ 单击“下一步”按钮，显示“保存安全策略”界面。保存之后，即可将该安全策略应用到当前或其他服务器上。单击“下一步”按钮，显示如图 1-30 所示的“安全策略文件名”对话框。在保存安全策略文件的路径之后输入安全策略文件名，根据需要输入相关的描述信息。



提示：单击“包括安全模板”按钮，还可以向当前安全策略中添加其他安全模板中的安全规则，这些规则将拥有较高的优先级。SCW 回滚功能将无法回滚已经应用的策略模板中的规则设置。



图 1-29 “审核策略摘要”界面



图 1-30 “安全策略文件名”界面

⑲ 单击“下一步”按钮，显示如图 1-31 所示的“应用安全策略”界面。如果选择“现在应用”单选按钮，则可以将安全策略立即应用到当前服务器；建议选择“稍后应用”单选按钮，测试之后再应用到服务器。

⑳ 单击“下一步”按钮，显示如图 1-32 所示的“正在完成安全配置向导”界面。单击“完成”按钮，完成安全策略的设置。

2. 应用安全配置策略

安全配置向导创建的安全策略可直接应用于所有运行 Windows Server 2008 或者 Windows Server 2003 SP1/SP2/R2 操作系统的网络服务器。大规模应用安全策略之前必须经过严格测试，确认可行之后方可部署。应用安全配置策略之后，必须重新启动计算机才可以生效。应用安全策略的主要操作步骤如下。



图 1-31 “应用安全策略”界面

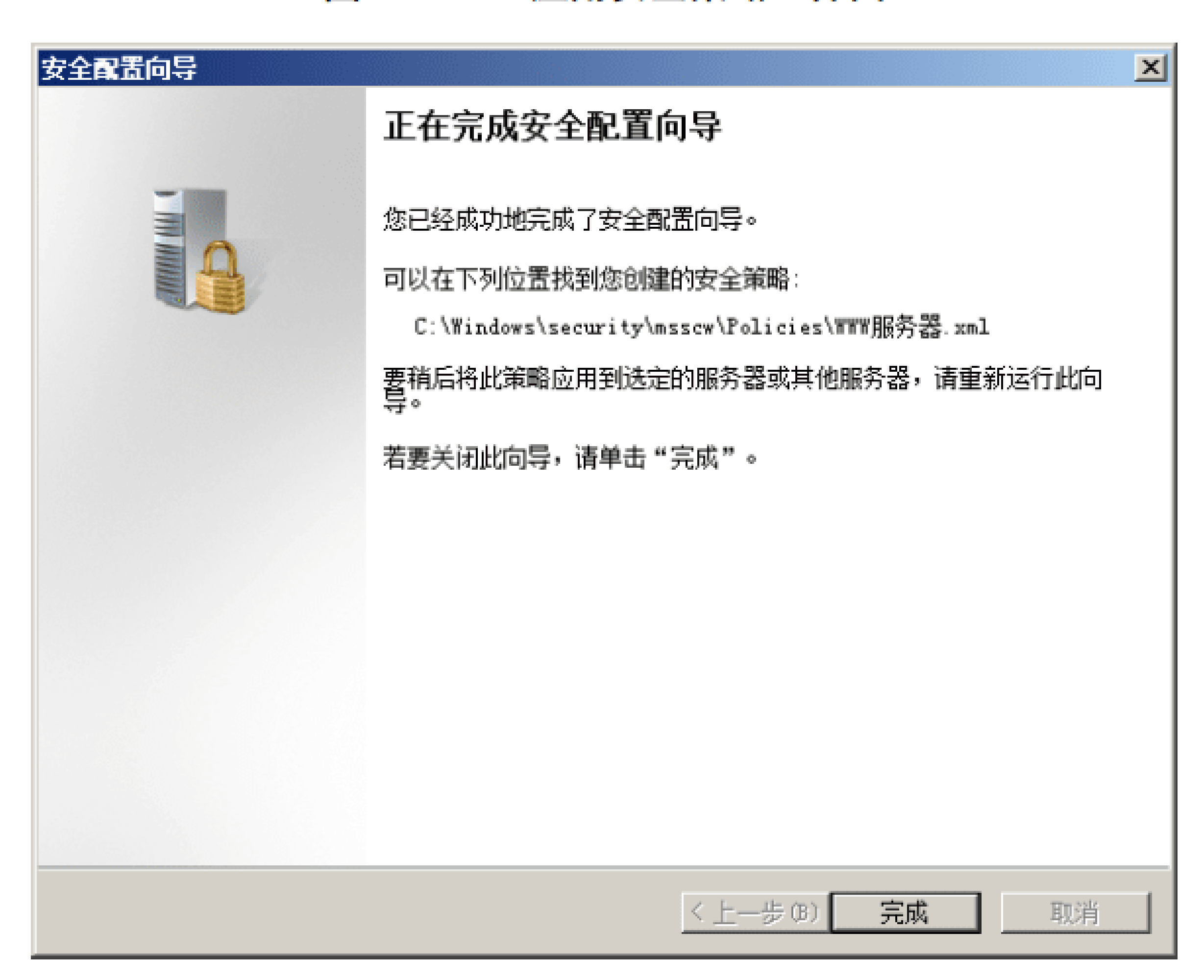


图 1-32 “正在完成安全配置向导”界面

① 依次单击“开始”→“管理工具”→“安全配置向导”，打开“安全配置向导”对话框，单击“下一步”按钮，在“配置操作”界面中，选择“应用现有安全策略”单选按钮，在“现有安全策略文件”文本框中输入安全策略文件的路径，也可单击“浏览”按钮查找，如图 1-33 所示。

② 单击“下一步”按钮，显示如图 1-34 所示的“选择服务器”界面，在“服务器”文本框中，输入想要应用到的服务器名称或 IP 地址。如果目标服务器为远程主机，则应单击“指定用户账户”按钮，选择连接到指定主机部署安全策略使用的用户账户及凭证。

③ 单击“下一步”按钮，显示如图 1-35 所示的“应用安全策略”界面，在“安全策略描述”列表框中显示的是该策略的相关描述信息，也可以单击“查看安全策略”按钮打开“SCW 查看器”窗口，查看其详细信息。单击“下一步”按钮，显示“正在应用安全策略”界面。将安全策略应用到本地计算机大概需要几分钟时间，应用到远程计算机时所需时间可能更长一些。

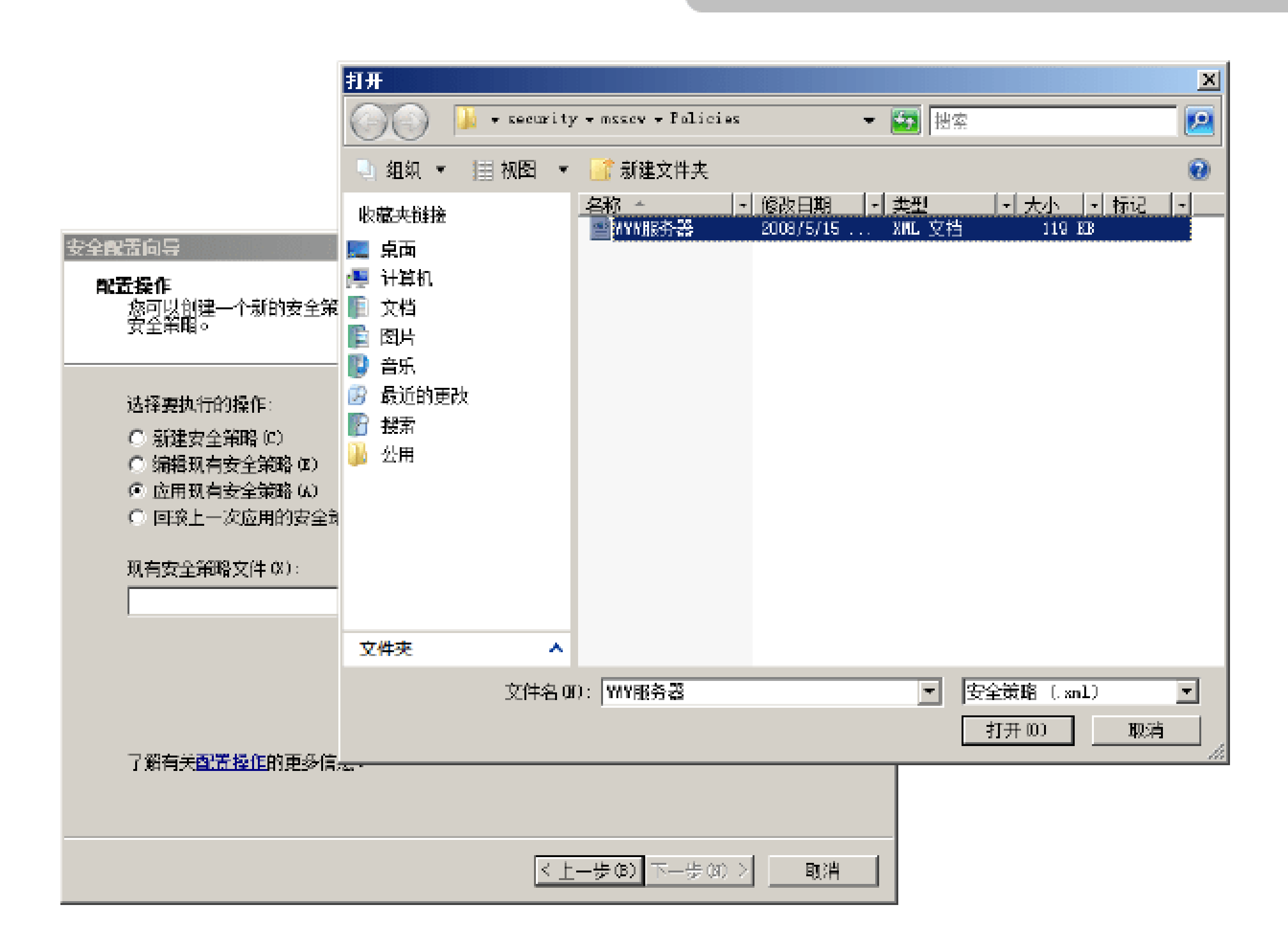


图 1-33 应用安全配置策略

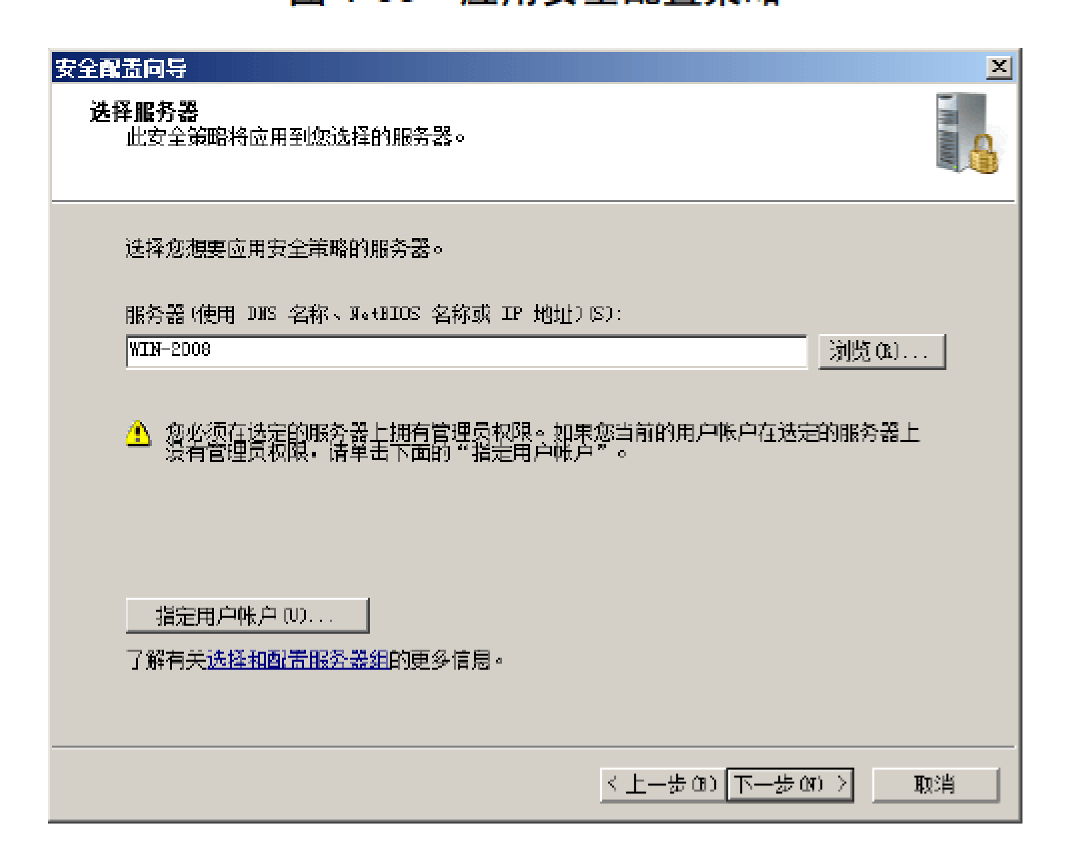


图 1-34 “选择服务器”界面

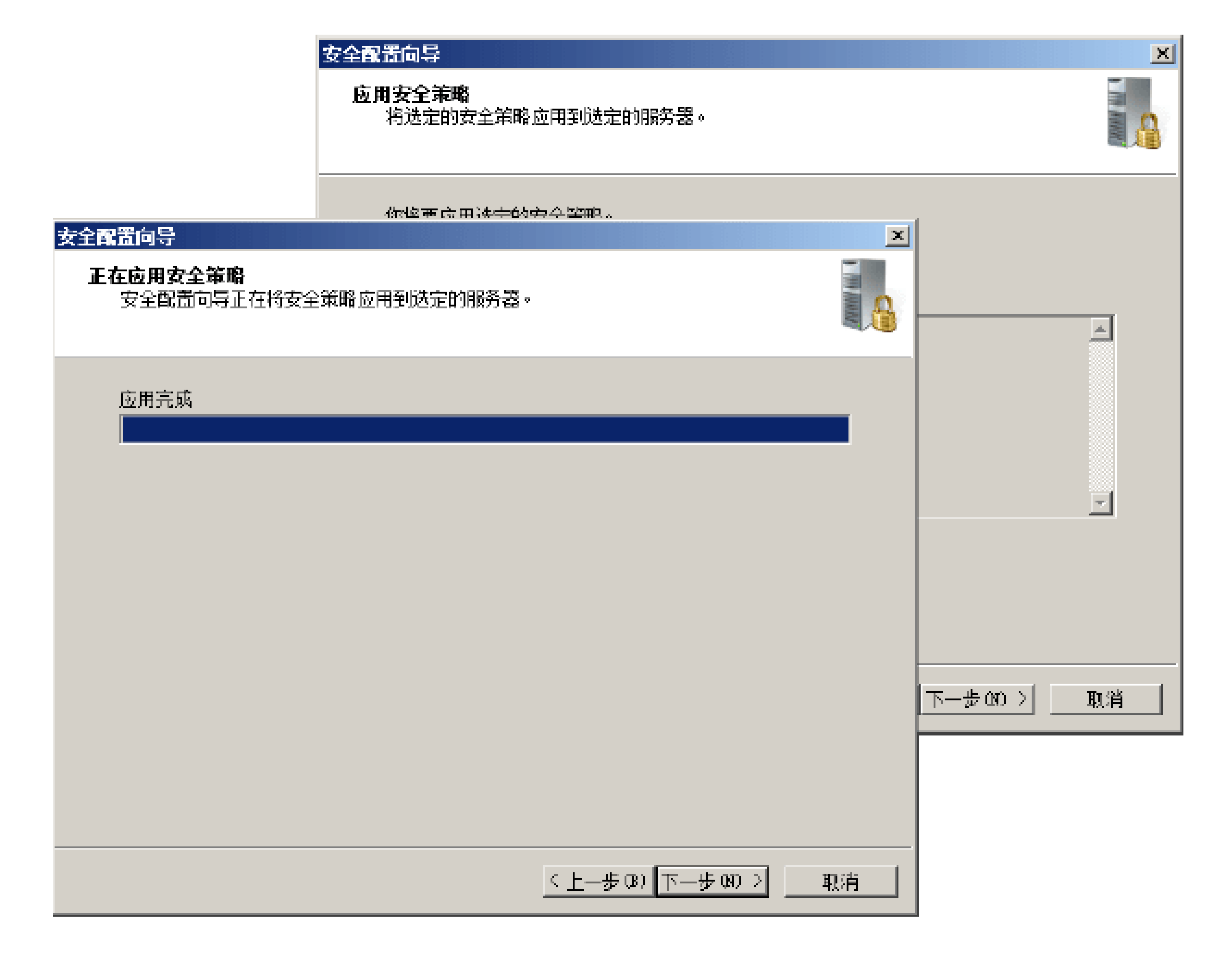


图 1-35 “应用安全策略”和“正在应用安全策略”界面

④ 单击“下一步”按钮，显示如图 1-36 所示的“正在完成安全配置向导”界面。

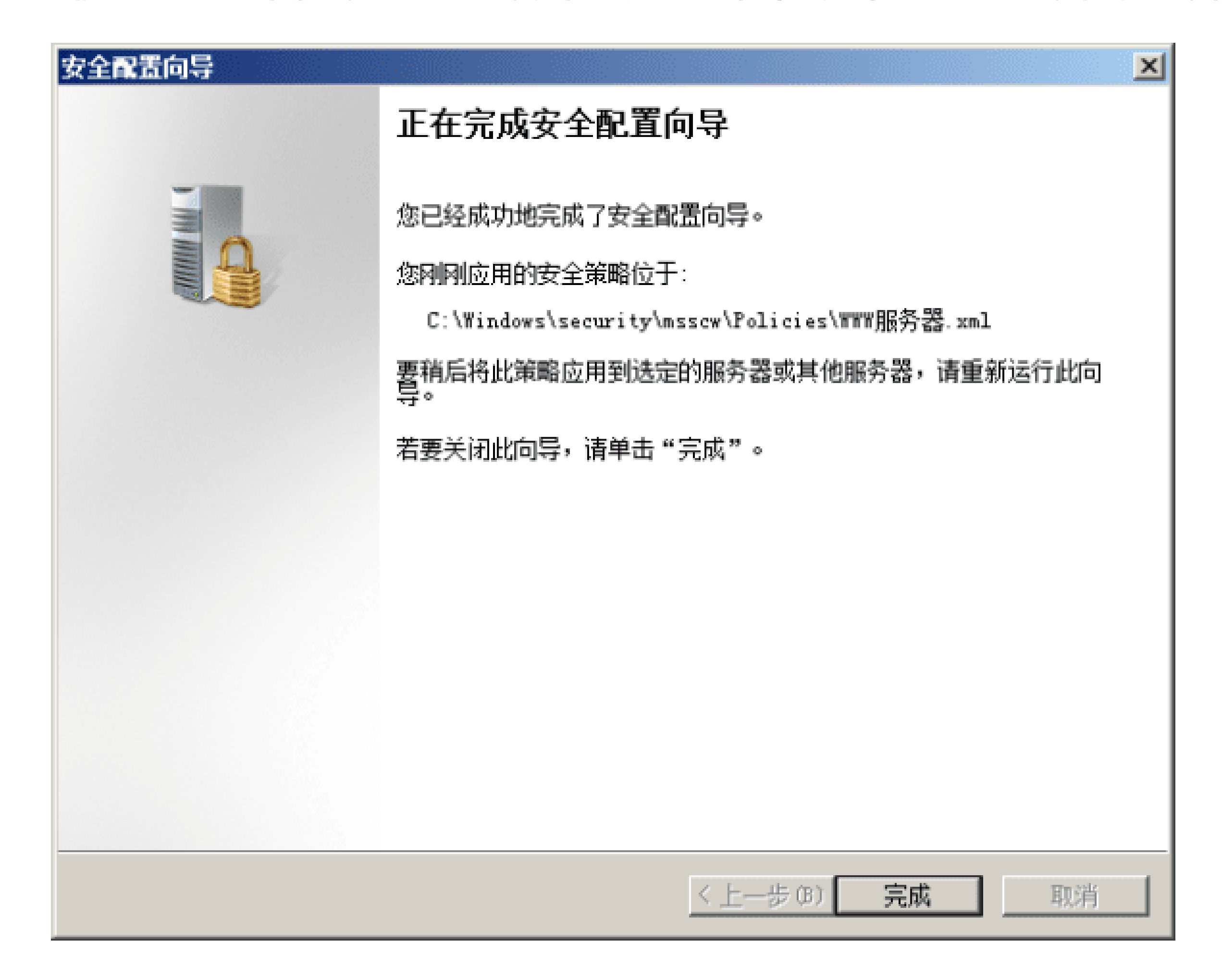


图 1-36 “正在完成安全配置向导”界面

⑤ 单击“完成”按钮，关闭安全配置向导。重新启动计算机后，应用的安全策略即可生效。

1.3 Windows Server 2008 被动防御安全

被动防御安全系统主要用于防范入侵 Windows Server 2008 系统的木马、病毒或间谍软件，这些都是影响系统安全的重要方面。防病毒系统主要用于扫描和清除计算机病毒，保护计算机系统和应用程序免遭病毒的侵害。防间谍系统则可以帮助系统避免间谍软件的入侵，从而保护重要的系统数据和用户信息。

1.3.1 配置防病毒系统

病毒对于计算机的危害性是不言而喻的，轻则造成应用程序出错、数据丢失，重则导致系统瘫痪，甚至波及网络中的其他计算机。为了避免病毒对系统的破坏，应注意如下事项：

- 服务器投入应用之前必须安装防病毒软件，并升级最新的病毒库。
- 确认防病毒软件来源的合法性、完整性以及可升级性。
- 应用过程中，应确保防病毒系统处于开启状态。
- 刚安装完成的操作系统，应进行一次完整的病毒扫描。
- 查看防病毒产生的日志文件。在系统运营后，经常查看病毒软件产生的日志文件。

1. 计算机病毒简介

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。病毒并非总是破坏文件或计算机，但它们通常会影响计算机的性能和稳定性。

计算机病毒通常具有如下特性：

- 传染性。

- 隐蔽性。
- 潜伏性。
- 破坏性。
- 表现性。

2. 单机防病毒系统

单机防病毒系统主要是指单个用户计算机上安装的病毒查杀软件，不必接受指定服务器的管理，通常都是通过 Internet 连接到官方服务器下载最新病毒库。单机防病毒系统成本相对较低，实现简单，易于管理，适用于小型企业局域网或 SOHO 网络。目前，针对单机用户的防病毒软件很多，建议用户通过正规渠道购买正版软件，或者登录相关软件的官方网站，下载试用版或共享版。

(1) 瑞星 2008

瑞星杀毒软件是国内反病毒软件中众多计算机生产商首选的杀毒软件，目前最新版本是瑞星杀毒软件 2008，它集病毒防范、病毒扫描、查杀于一身，具有扫描速度快、识别率高、占用资源少等优点。瑞星杀毒软件不仅可以保护计算机系统不受病毒入侵，而且发现感染病毒后，还可以进行自动清除。瑞星杀毒软件可以运行于 Windows Server 2008 或 Windows Server 2003 等服务器平台。如图 1-37 所示，是瑞星杀毒软件 2008 的主窗口。



图 1-37　“瑞星杀毒软件”主窗口

(2) NOD32

NOD32 是 ESET 公司的防病毒产品，以应用平台广泛著称，支持的平台包括 DOS、Windows 9x/NT/2000/XP/2003/Vista/2008，以及 Novell Netware Server、Linux、BSD 等。对于 Windows 版本，它同时支持 32 位和 64 位平台，包括 Windows Vista 和 Windows Server 2008。NOD32 在线监测功能严密，占用内存资源较少，清除病毒的速度和效果都令人满意。如图 1-38 所示是 NOD32 单机版主窗口。

(3) Windows Live OneCare

Windows Live OneCare 是微软公司推出的首款杀毒软件套件，包括反病毒防火墙、数据备份、反间谍、磁盘清理等功能，几乎可以覆盖所有的个人安全领域。随着时间的推移，相信会更加适合于 Windows 服务器。Windows Live OneCare 这项全面的服务可以帮助您保护计算机免受许多不同种类的威胁，还可以帮助您在紧急情况下备份重要文档，并定期调整计算机从而帮助计算机稳定运行。如图 1-39 所示是 Windows

Live OneCare 主窗口，需要注意的是，目前仅能在英文版 Windows 操作系统中使用。

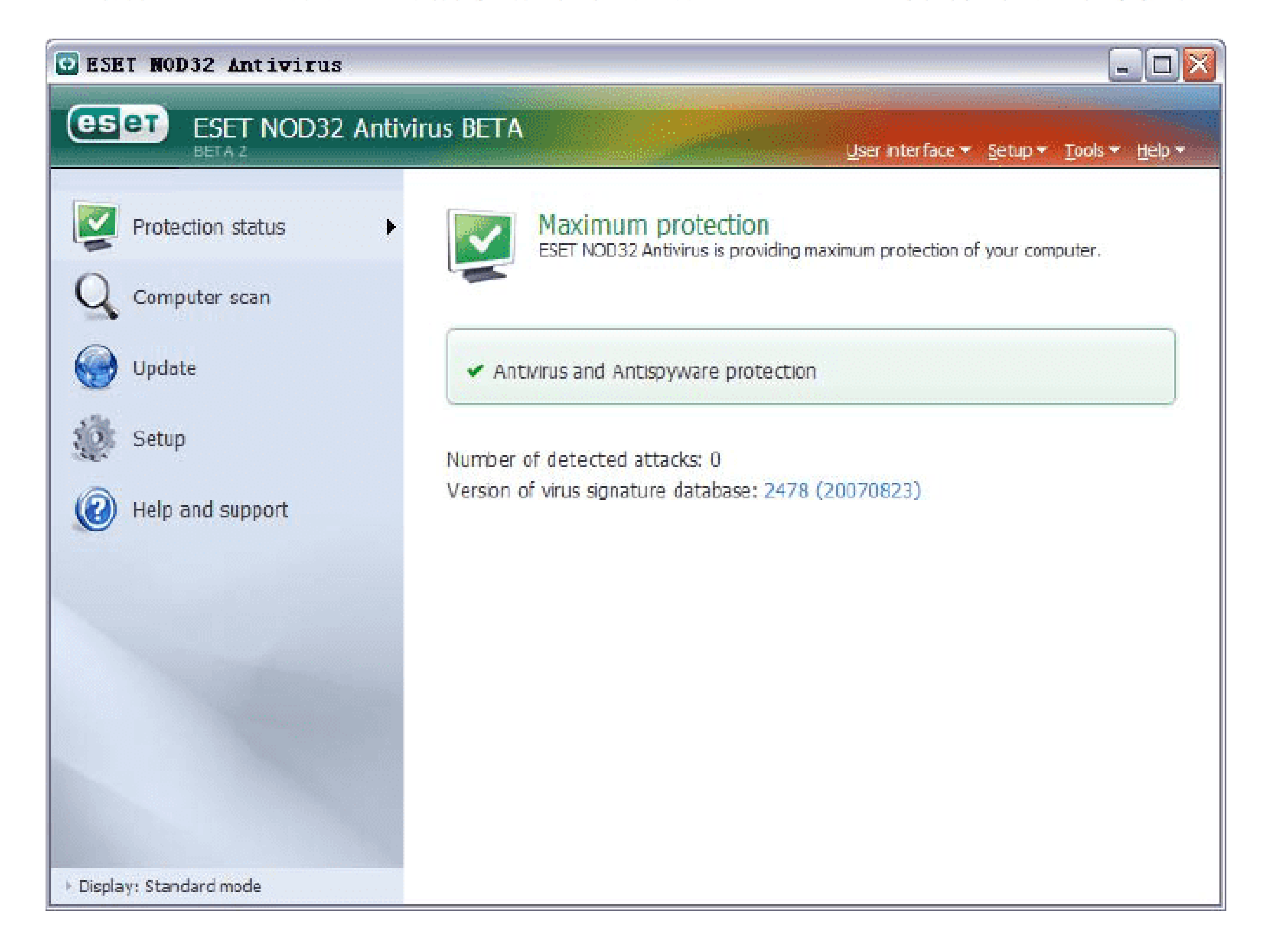


图 1-38　NOD32 单机板主窗口

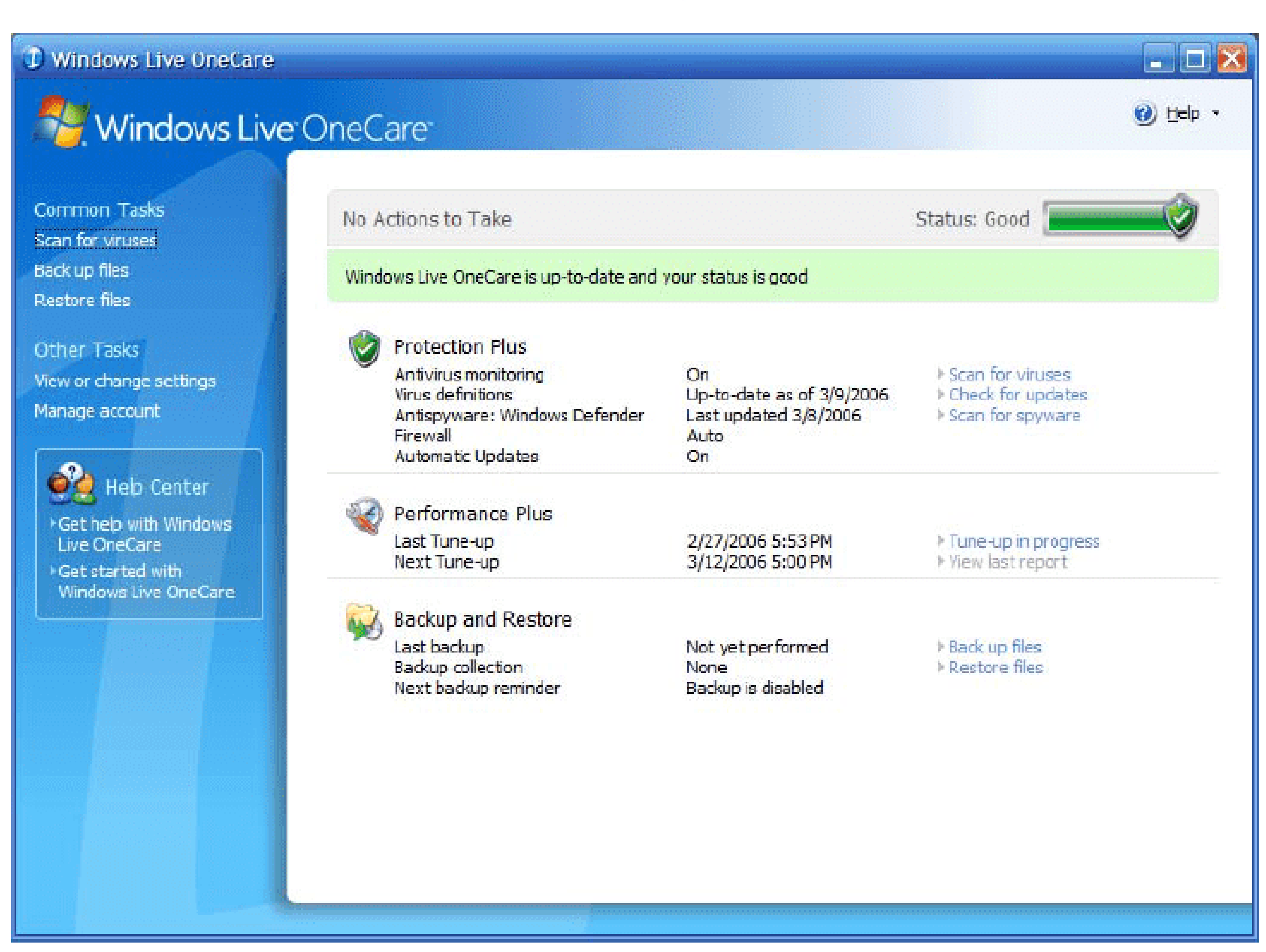


图 1-39　Windows Live OneCare 主窗口

3. 网络防病毒系统

网络防病毒系统主要应用于大、中型企业网络的病毒防御工作，相对于单机防病毒软件而言，不仅防御范围广、功能强大，而且可管理性强。目前，广泛应用的企业杀毒软件有 Symantec AntiVirus 企业版、瑞星杀毒软件企业版、McAfee 网络防病毒软件等。网络防病毒系统主要由服务器和客户端两部分组成。主要特点就是客户端可以直接通过局域网从服务器获得最新的病毒库升级文件，并且管理员可以通过防病毒服务器客户端监控功能，及时了解客户端的运行情况，以便统一管理和部署。因此，部署企业杀毒软件系统不仅可以节省整个网络的带宽开销，还可以提高网络安全性。如图 1-40 所示是大多数企业杀毒软件的运

行模式。

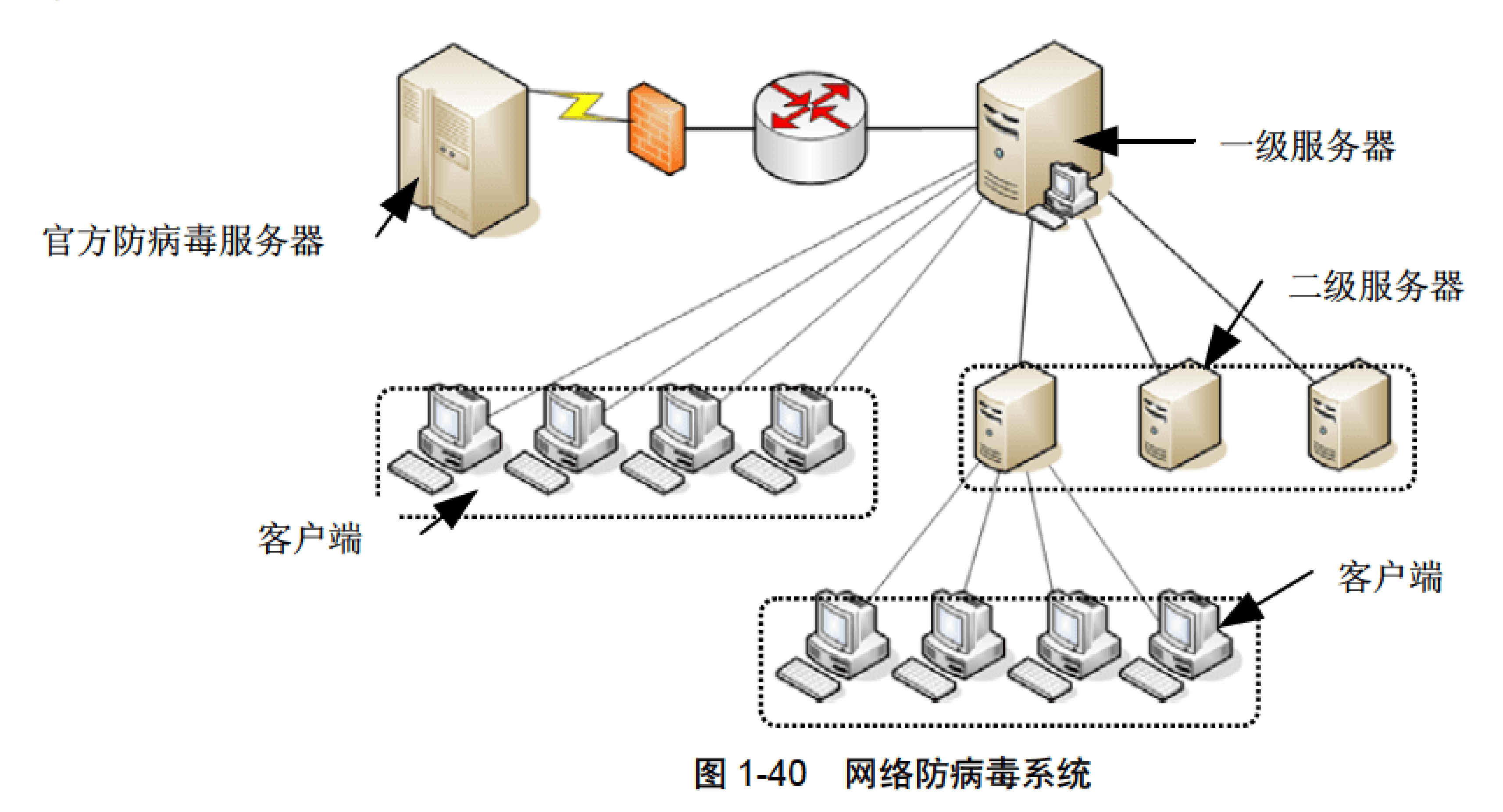


图 1-40　网络防病毒系统


提示：有关网络防病毒系统部署的详细介绍，请参考本书“第 14 章 Windows 防病毒服务”中的相关内容。

(1) 服务器端

企业杀毒软件系统中的服务器端是指安装服务器管理软件的计算机，可以直接登录杀毒软件官方升级服务器，快速下载最新病毒库文件。管理员可以通过服务器端对下属的二级服务器、客户端等进行统一管理，如分发升级文件、接收客户端病毒报警、实时状态监控等。另外，服务器端通常都集成适用于各种版本操作系统的客户端安装程序，管理员可以直接通过局域网安装客户端，免去一一安装的麻烦。

(2) 客户端

客户端是指接受网络防病毒服务器管理的所有计算机，必须安装与服务器端配套的杀毒软件，并接受服务器的管理。客户端既可手动连接到局域网防病毒服务器、更新病毒库，也可以指定为自动接收来自服务器的病毒库文件。

1.3.2　配置防间谍系统

间谍软件通常是指自动安装，或者未提供足够通知、同意或控制的情况下，就在计算机上运行的应用程序。一般情况下，间谍软件在感染计算机后可能不会显示任何症状，但许多类型的恶意软件或不需要的程序都可以影响计算机的运行方式，如监视用户的实时行为、收集用户信息等。目前的防间谍软件产品很多，应根据实际情况选择一款适合自己使用的防间谍软件产品，同时注意软件来源的合法性和安全性，以及间谍软件代码更新库的升级能力。

1. 如何避免间谍软件

间谍软件和木马相比，实现原理和方法更多。间谍软件通常有两种主要行为：第一，监视应用程序运行，收集重要数据并发送到软件另一端的操纵者；第二，通过捕捉 IE 的主页和搜索页面的设置来改变目标系统的行为，例如，擅自修改主页、弹出广告页面等。从系统安全的角度考虑，用户必须重视识别间谍软件、杜绝间谍软件。

(1) 定期运行反间谍软件

反间谍软件可以定期进行扫描以发现隐藏的间谍软件，例如 Ad-Aware，Spybot 等。在 Windows Server 2008 中，用户可以通过配置系统内置的 Windows Defender，避免间谍软件的入侵。

(2) 避免通过 P2P 方式下载文件

不要通过 P2P 下载任何可疑文件，尤其是可执行程序或压缩包，将间谍软件同其他文件进行捆绑，是其主要传播途径之一。

(3) 关闭邮件的预览功能

如果电子邮件中包含间谍软件，则打开或预览邮件内容的同时，可能激活间谍程序。关闭预览面板的预览功能，这样可以在不打开的情况下就直接删除信息。

(4) 安装软件之前仔细阅读 EULA

在安装软件之前，请仔细阅读终端用户许可协议(EULA，End User License Agreements)，因为有些终端用户许可协议会告诉你如果安装了本软件，也就同时决定安装这个软件中带有的间谍软件。另外还要查看一些独立的信息源，因为有些终端用户许可协议不会告诉你有间谍软件的存在。

(5) 合理设置 IE 浏览器的安全级别

IE 浏览器为用户提供了多个安全级别，通常情况下，严格的安全级别可以限制大部分通过 IE 入侵的间谍软件，建议设置为中级，甚至高级安全级别，禁止浏览器安装任何你没有要求的 ActiveX 控件。

2. 部署防间谍软件注意事项

在安装防间谍软件时应注意如下事项：

- 建议配置成系统启动时自动启动防间谍软件。
- 定制自动更新间谍软件代码库。
- 定制在指定时间之内扫描系统的完整信息。
- 启动实施监视系统。
- 定制应用程序许可策略。
- 保存并定期察看日志信息。

3. Windows Defender

为了应对网络中泛滥的木马、间谍等恶意软件对系统安全的挑战，微软也推出了反木马、间谍软件的专用程序 Windows Defender。Windows Defender 的前身是 Giant 公司的 Giant Antispyware，微软将该公司收购后便将其更名为 Windows Defender。

(1) Windows Defender 概述

Windows Defender 是微软公司提供的一款免费组件，并且在 Windows Vista 和 Windows Server 2008 系统中，Windows Defender 已经成为系统默认安装的安全组件之一。Windows Defender 具有如下主要功能。

- 提供完备的恶意软件清除功能：Windows Defender 在扫描查杀的同时，还会对恶意软件添加的文件以及修改的注册表内容进行同步检测和删除，清除比较干净。
- 与杀毒软件相得益彰：Windows Defender 是设计用来检测、删除或隔离用户电脑中的已知或可疑间谍软件的安全防御工具，针对的是杀毒工具无法处理的恶意软件，所以并不会和系统中安装的防病毒软件冲突，相反两者配合工作，安全防御效果会更好。

- 提供多种灵活扫描方式：Windows Defender 提供如下 3 种扫描方式，用户可根据实际需要选择。
  - Quick Scan：它可以扫描间谍软件常用的安装目录，可以在最短的时间里发现大多数间谍软件。
  - Full Scan：它可以扫描计算机中的全部硬盘分区以及全部文件夹。这种扫描方式非常彻底，但是耗时较多，具体的耗时根据用户的硬盘大小以及文件多少来决定。另外，扫描过程中，系统的整体运行速度会有所下降。
  - Custom scan：在这种方式下，用户可以选择所要扫描的硬盘分区和文件夹。如果 Windows Defender 在这种模式下发现了间谍软件，将进而启动 Quick Scan 模式对间谍软件进行清除或隔离。
- 实时监控功能：Windows Defender 最大的特点在于当恶意软件试图入侵计算机时，会自动提醒用户。需要注意的是，只有当恶意软件是与其他软件捆绑安装时，Windows Defender 才会警报提醒，而当直接安装恶意软件时，则不会表现任何动作。
- 管理员可以监控用户行为：管理员可以允许用户使用 Windows Defender 扫描计算机，在发现可疑程序后选择相应的执行动作，以及查看 Windows Defender 的活动记录。管理员还可以限制 Windows Defender 的管理权限。在默认情况下，任何用户都可以使用 Windows Defender。

(2) 配置 Windows Defender 选项

如果不希望每次都使用 Windows Defender 的默认设置扫描系统，可以在 Windows Defender 窗口中，单击“工具”按钮进行自定义配置，打开“工具和设置”对话框，继续单击“选项”链接，打开如图 1-41 所示的窗口，在这里可以设置包括自动扫描、实时保护选项、默认操作、管理员选项等在内的 Windows Defender 高级选项。

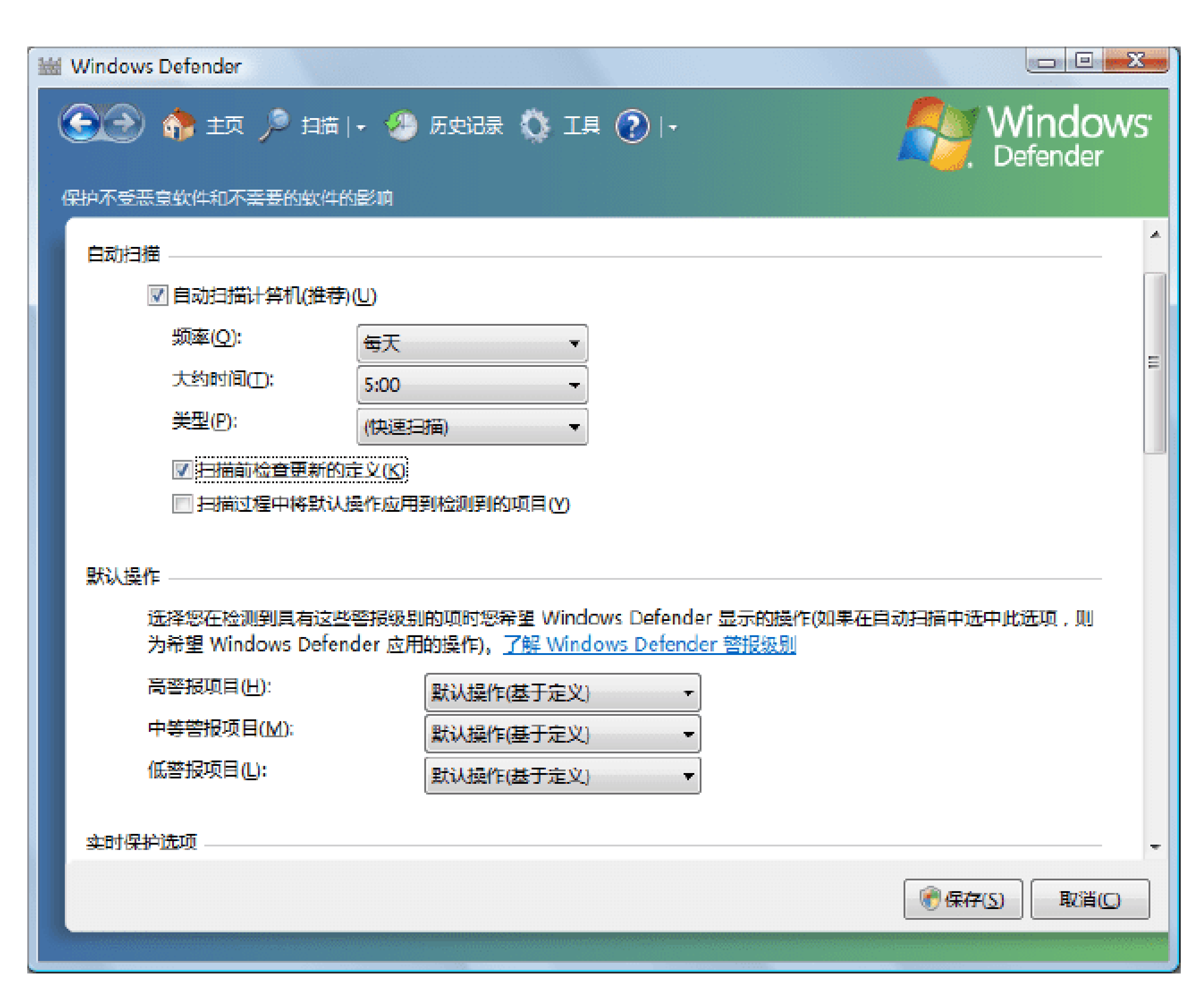


图 1-41 配置 Windows Defender 选项

- 自动扫描：在“自动扫描”选项区域，选中“自动扫描计算机”复选框，然后设置适当的扫描频率(如每天、每周等)和执行扫描的时间，并在“类型”下拉列表中选择希望执行的扫描方式即可。建议选中“扫描前检查更新的定义”复选框，以便确保 Windows Defender 定义库的最新状态。
- 默认操作：在“默认操作”选项区域中，可设置在不同警报级别下所执行的操作。Windows Defender 默认提供 3 种警报等级，分别为高警报项目、中等警报项目和低警报项目。用户可以根据需要为

每一种警报等级的项目设置不同的操作，如对于扫描过程中发现的“高警报项目”，可以直接将默认操作定义为“删除”，对于低警报项目则可以设置为“忽略”。

- 高警报项目。可能搜集个人信息并对您的隐私产生负面影响或损害计算机的程序，例如，通常在未经用户允许的情况下，搜集信息或更改设置。建议立即删除此类项目。
- 中等警报项目。可能影响用户的隐私或更改计算机对计算体验产生负面影响的程序，例如，搜集个人信息或更改设置。对于此类项目，建议用户复查警报详细信息，查看为何会检测到此软件。如果不喜欢软件的操作方式，或如果不了解和信任发行者，则考虑阻止或删除此类项目。
- 低警报项目。可能不需要的软件会搜集有关用户或计算机的信息，或更改计算机的运行方式，但它按照协议操作，安装时会显示许可条款。此类项目应视情况而定，如果安装之前提示相关信息及安装结果，则可以保留。如果不能确定信任该软件的发行者，则建议删除。

■ 实时保护选项：在如图 1-42 所示的“实时保护选项”区域中，选中“使用实时保护”复选框，即可启用 Windows Defender 实时保护功能。Windows Defender 实时保护的项目包括系统配置、Internet Explorer 加载项、Internet Explorer 配置、服务和驱动程序、应用程序执行、应用程序注册、Windows 加载项等。默认情况下，Windows Defender 已经对所有安全代理组件开启实时保护功能。

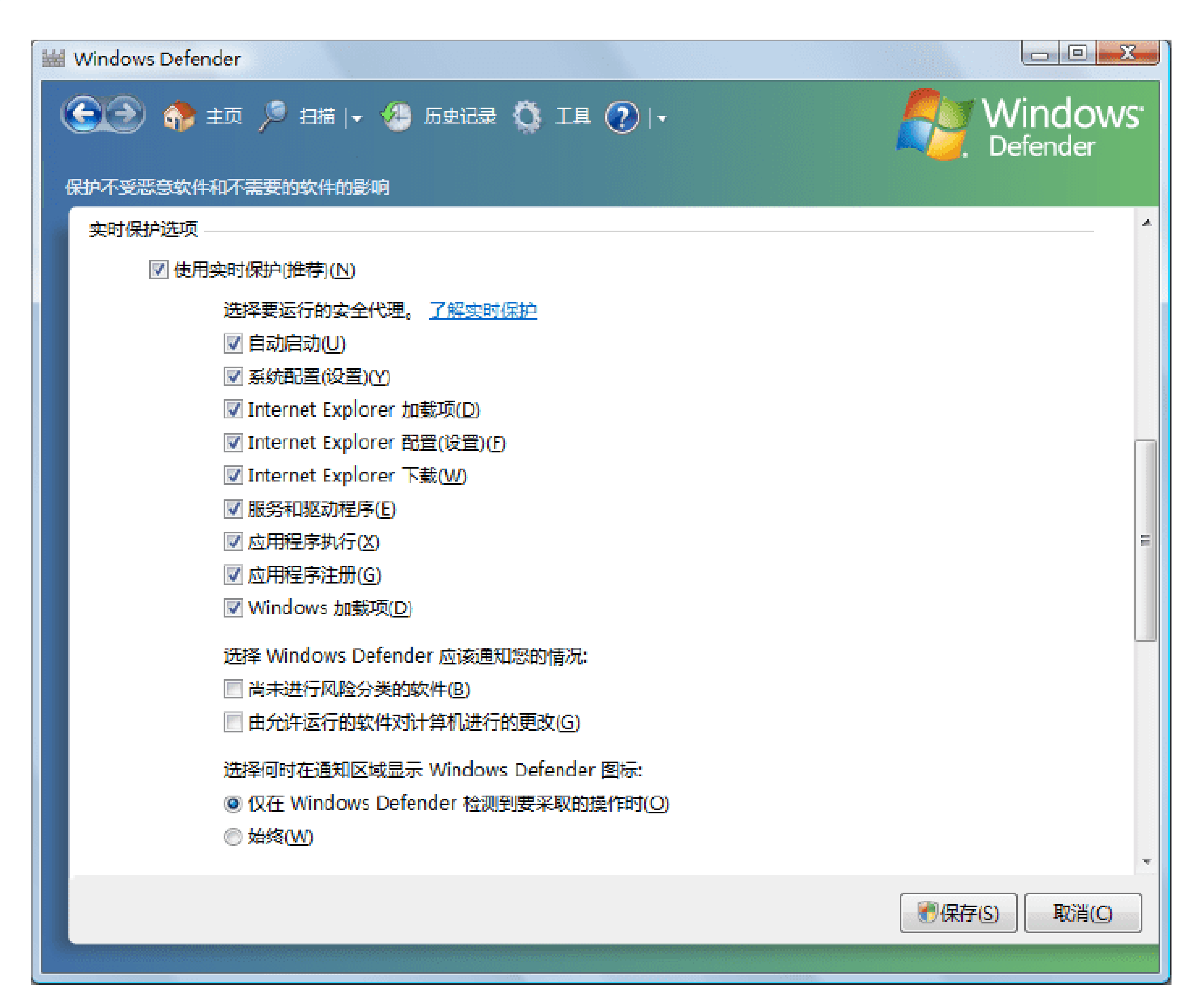


图 1-42　实时保护选项

■ 高级选项：在如图 1-43 所示的“高级选项”选项区域中，用户可以对 Windows Defender 扫描时的如下 4 个高级选项进行设置：

- 扫描存档文件和文件夹内容是否存在潜在的威胁。扫描这些位置可能会延长扫描时间，但间谍软件和其他可能不需要的软件会自行安装并试图“隐藏”在这些位置中。
- 使用启发式检测尚未分析风险的软件的有害或不需要的行为。Windows Defender 使用定义文件识别已知威胁，但它还可以检测未在定义文件中列出的软件的可能有害或不需要的行为，

并向用户发出警报。

- 在对检测到的项应用操作之前创建还原点。由于可以将 Windows Defender 设置为自动删除检测到的项目，因此如果要使用原本不想删除的软件，则可以选择此选项还原系统设置。
- 不要扫描这些文件或路径。使用此选项可以选择任何用户不希望 Windows Defender 扫描的文件和文件夹。

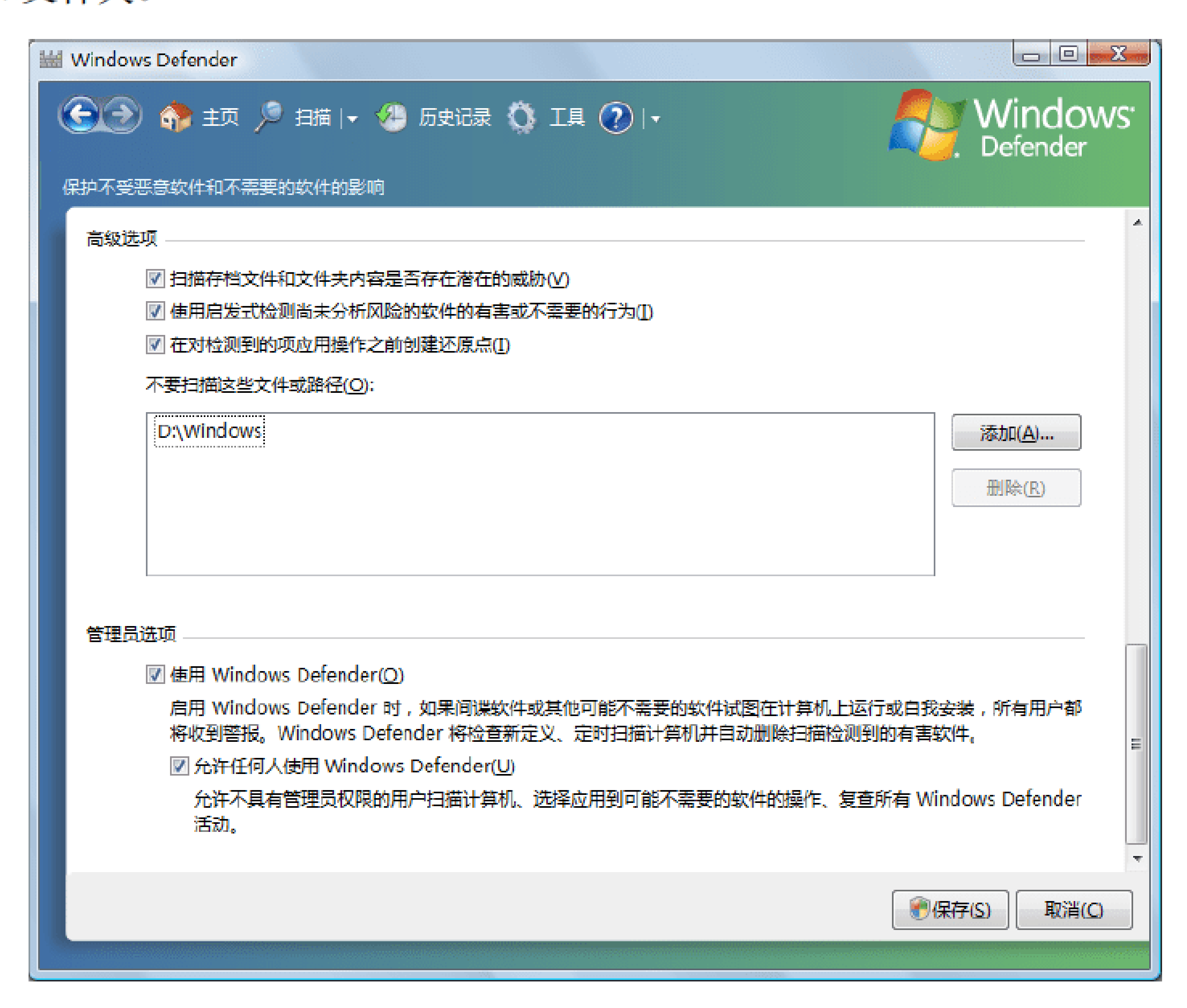


图 1-43　高级选项

- 管理员选项：在“管理员选项”区域中，选中“使用 Windows Defender”复选框，当间谍软件或其他潜在不安全的软件试图运行或安装在计算机上时，用户将收到 Windows Defender 发出的警报；若选中“允许任何人使用 Windows Defender”复选框，则允许没有管理员权限的用户使用 Windows Defender。

(3) 更新 Windows Defender 定义库

使用 Windows Defender 时，保持其定义库处于最新状态是非常重要的。定义是一些文件，其中包含了已知间谍软件和其他可能不需要的软件的特征代码，类似于防病毒程序的病毒库。由于间谍软件在不断发展，Windows Defender 依靠更新定义来确定正尝试在计算机上安装、运行或更改设置的软件是否为可能不需要的软件或恶意软件。

在配置 Windows Defender 自动扫描时，如果选中“扫描前检查更新的定义”复选框，即可将其配置为自动更新定义。除此之外，用户还可以通过手动方式更新 Windows Defender 定义库。在 Windows Defender 窗口中，单击“帮助”按钮旁边的箭头，并选择“检查更新”即可。为确保计算机安全，Windows Defender 会在定义文件过期超过 7 天未更新时通知用户，此时直接单击“立即检查更新”按钮即可。显示如图 1-44 所示。

(4) 注意事项

默认情况下，服务器系统都是使用最小方式安装的，所以 Windows Defender 组件不会出现在控制面

板中。管理员可以通过“管理服务器”控制台，启动“添加功能向导”对话框，在“功能”列表框中，选中“桌面体验”组件并安装，如图 1-45 所示。安装完成后即可配置和使用 Windows Defender。

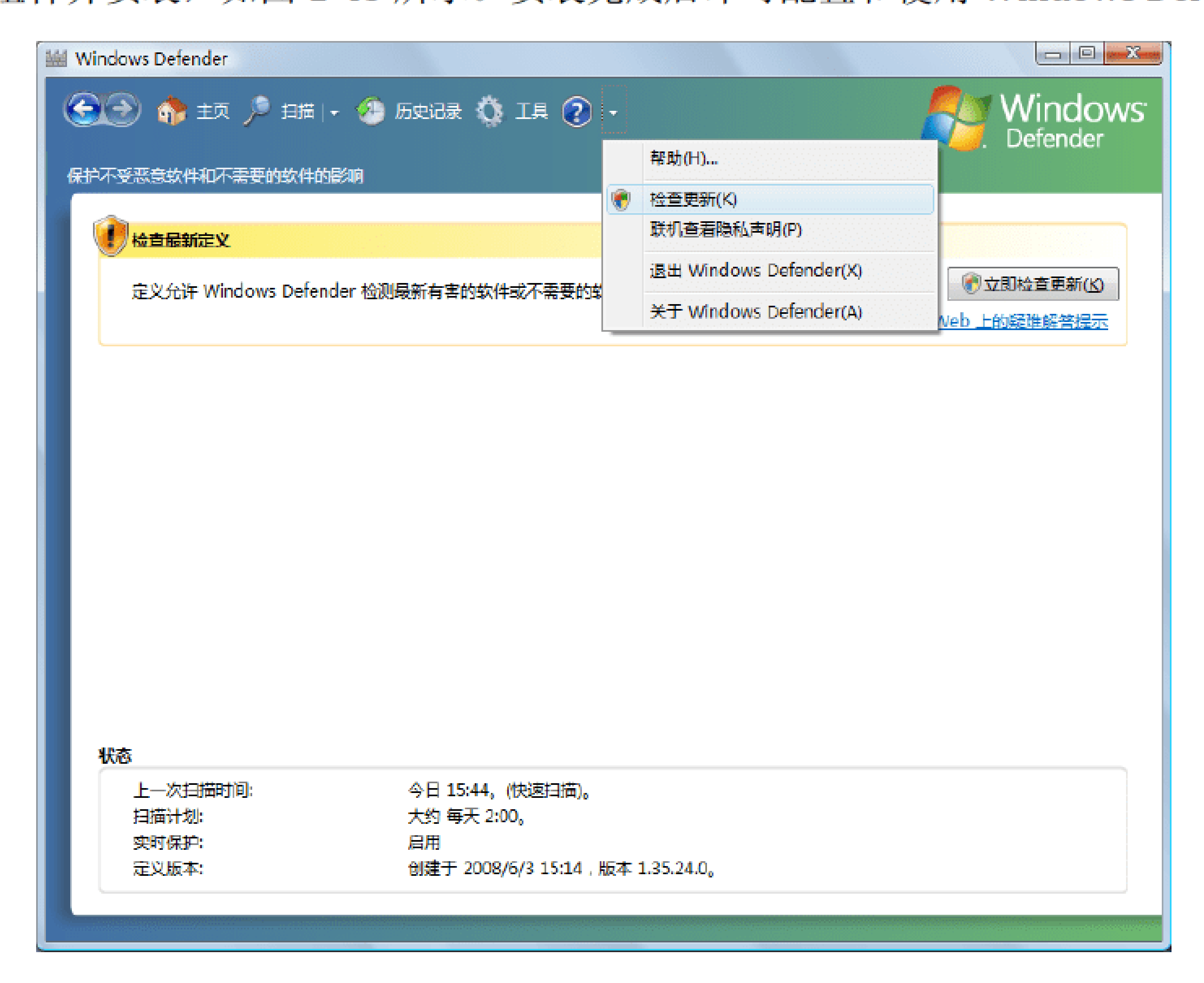


图 1-44　更新 Windows Defender



图 1-45　“添加功能向导”对话框

1.4　Windows Server 2008 系统安全

Windows Server 2008 系统提供的系统安全涉及诸多方面，例如，应用程序安全、注册表安全、系统服务安全、文件权限安全、用户账户安全、活动目录安全、注册表安全、组策略安全、端口安全、网络服

务安全等。任何一处隐藏的系统安全漏洞，都可能会招致整个系统安全的灭顶之灾。

1.4.1 应用程序安全

在服务器上安装正常使用的应用程序(包括更新的 IE 浏览器版本)，同时安装配置选择好用来提供网络服务的程序(例如 IIS 服务、FTP 服务、SQL Server 数据库服务等)。非必要运行服务器操作系统的计算机不要登录到 Internet。

在配置系统应用程序时，应注意以下事项：

- 不要安装任何多余的程序。服务器仅提供网络服务，不需要安装任何服务以外的程序。
- 安装服务和应用程序，尽量选择最新的安装版本，这样，通常可以保证没有近期发布的程序漏洞。不需要的应用程序服务尽量不要安装，或者配置为禁用模式。
- 通常不要在服务上运行系统提供的应用程序访问网络，服务器的漏洞有时会被恶意利用。
- 卸载安装 Windows Server 2008 过程中默认安装的画图、计算器等非必要应用程序，通常仅保留记事本或写字板即可。
- 建议删除甚至拒绝在服务器上安装 Microsoft Office 或者其他的日常办公软件。
- 不要在服务器上运行任何开发工具、软件调试器、扇区读写编辑器等可对操作系统底层进行操作的应用软件，可执行程序越少越好。
- 服务器设置严格的权限许可，共享文件的访问建议使用 ACL 权限控制。
- 对系统文件夹(x:\windows,x:\windows\system 等)使用 ACL 控制，避免赋予系统文件夹“写入”的权限。
- 服务器的 IP 地址设置为静态 IP。



注意：应了解要安装的程序是否存在缺陷，如 IE、Outlook、Media Player 等微软提供的程序可能含有漏洞。建议经常到微软的网站上查看最新的安全公告，或者接受微软的安全邮件列表。

1.4.2 系统服务安全

安装操作系统的同时，也会自动安装大量服务。但是，运行的服务越多，可能造成的安全漏洞也越多，同时还会占用大量的系统资源。而对于有能力利用服务特权和功能来访问本地 Web 服务器或其他网络服务器的不法入侵者来说，服务是最主要的漏洞点。不验证客户端身份的服务、使用不安全协议的服务、特权太多的服务等都将带来风险。服务越少、漏洞越少、系统越安全。

配置系统服务时应注意以下事项：

- 根据服务的描述以及业务的需求，确定是否使用此服务。
- 具体每个服务的内容和功能，请参考微软的说明和咨询业内安全专家。
- 禁止或者设置成手动启动的方式处理系统非必需的服务。
- 如对系统可能造成的影响不了解，在测试环境中测试验证通过以后，再在应用环境中部署。
- 对于安装应用程序同步安装的服务，如无必要，应将其关闭。

依次单击“开始”→“管理工具”→“服务”，即可打开“服务”控制台窗口，并列出本地计算机中所有的服务，如图 1-46 所示。

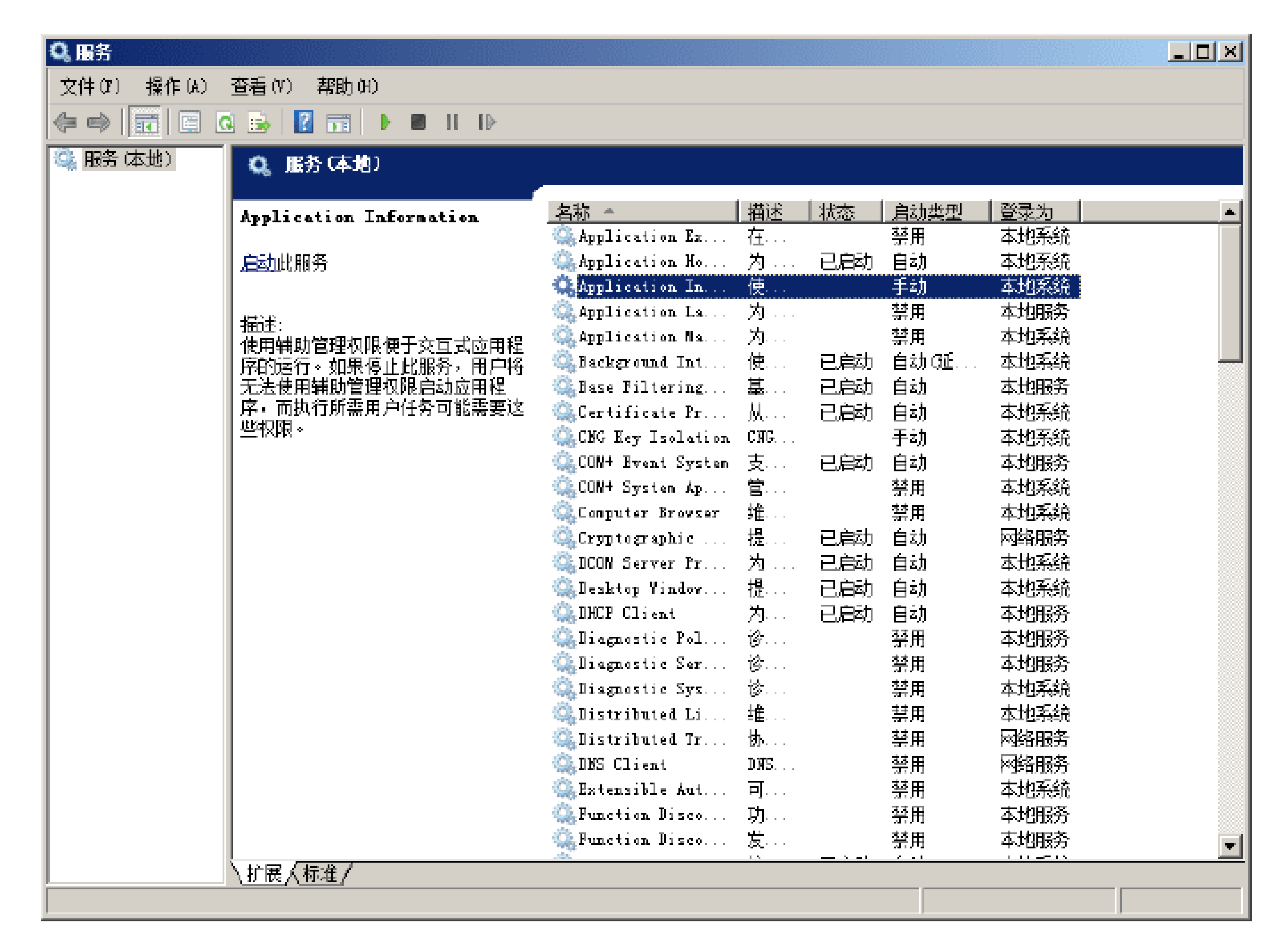


图 1-46　默认安装的服务列表

系统服务的处理不同于其他设置，因为所有服务的漏洞、对策及潜在影响在本质上都一样。第一次安装 Windows Server 2008 操作系统的时候，系统将在启动时创建并配置默认服务。有些服务在组织环境中并不需要，但仍在 Windows 中被启用，来确保应用程序或客户端兼容或辅助进行系统管理。

1.4.3　注册表安全

注册表中包含了 Windows 系统运行时所需的信息，例如，每个用户的配置文件、计算机上安装的应用程序及其设置、系统上存在哪些硬件以及正在使用哪些端口等。因此，注册表作为 Windows 系统中重要的配置文件，对系统安全起着决定性的作用。

1. 禁止注册表远程访问

Windows Server 2008 在默认安装时启用了允许远程访问注册表。需要注意的是，系统服务的启动、ACL 权限的修改、用户账户的创建，都可以在注册表中完成，因此开启此功能将会对系统安全带来极大的隐患，必须严格禁止使用远程注册表访问功能。该安全设置确定在网络上可访问哪些注册表路径和子路径。

① 打开组策略控制台，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，显示如图 1-47 所示的窗口。

② 在右侧的策略窗口中，双击“网络访问：可远程访问的注册表路径和子路径”策略，显示如图 1-48 所示的“网络访问：可远程访问的注册表路径和子路径 属性”对话框。

③ 删除列表框的所有数据，单击“确定”按钮保存设置。

④ 双击“网络访问：可远程访问的注册表路径”策略，显示如图 1-49 所示的“网络访问：可远程访问的注册表路径 属性”对话框。

⑤ 删除文本框的所有数据，然后单击“确定”按钮即可。



提示：编辑注册表不当可能会严重损坏的系统。在更改注册表之前，应备份计算机上任何有价值的数据。

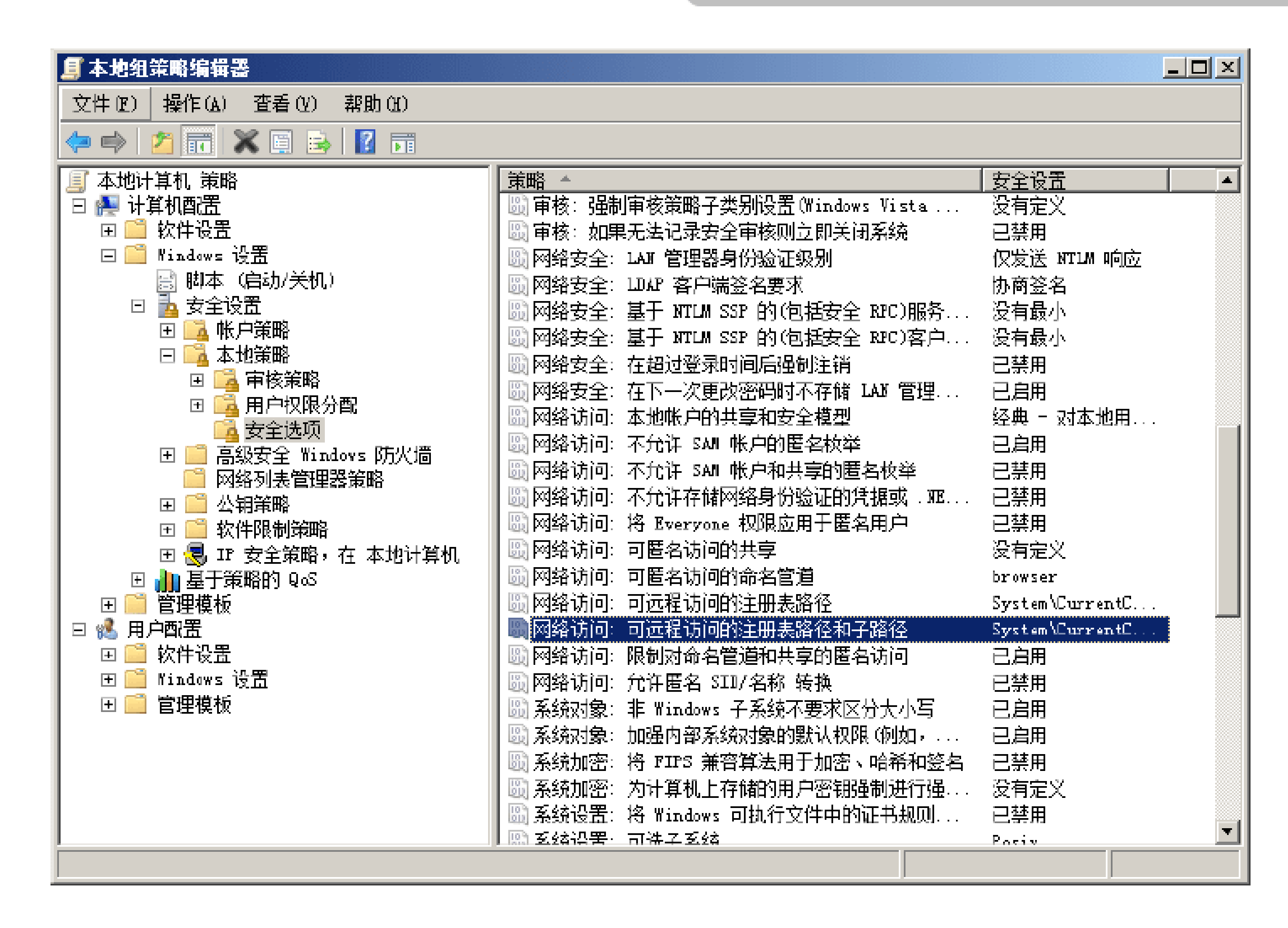


图 1-47　“本地组策略编辑器”窗口

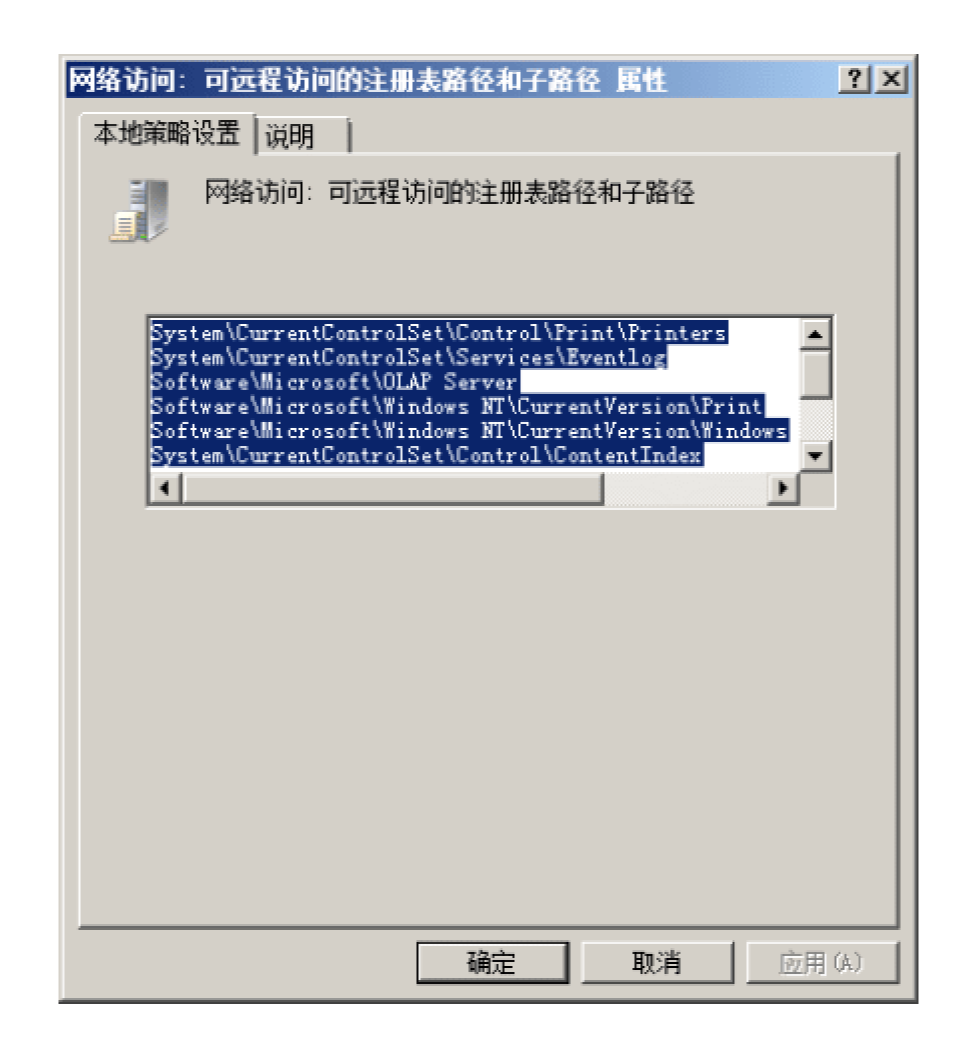


图 1-48　“网络访问：可远程访问的注册表路径和子路径 属性”对话框

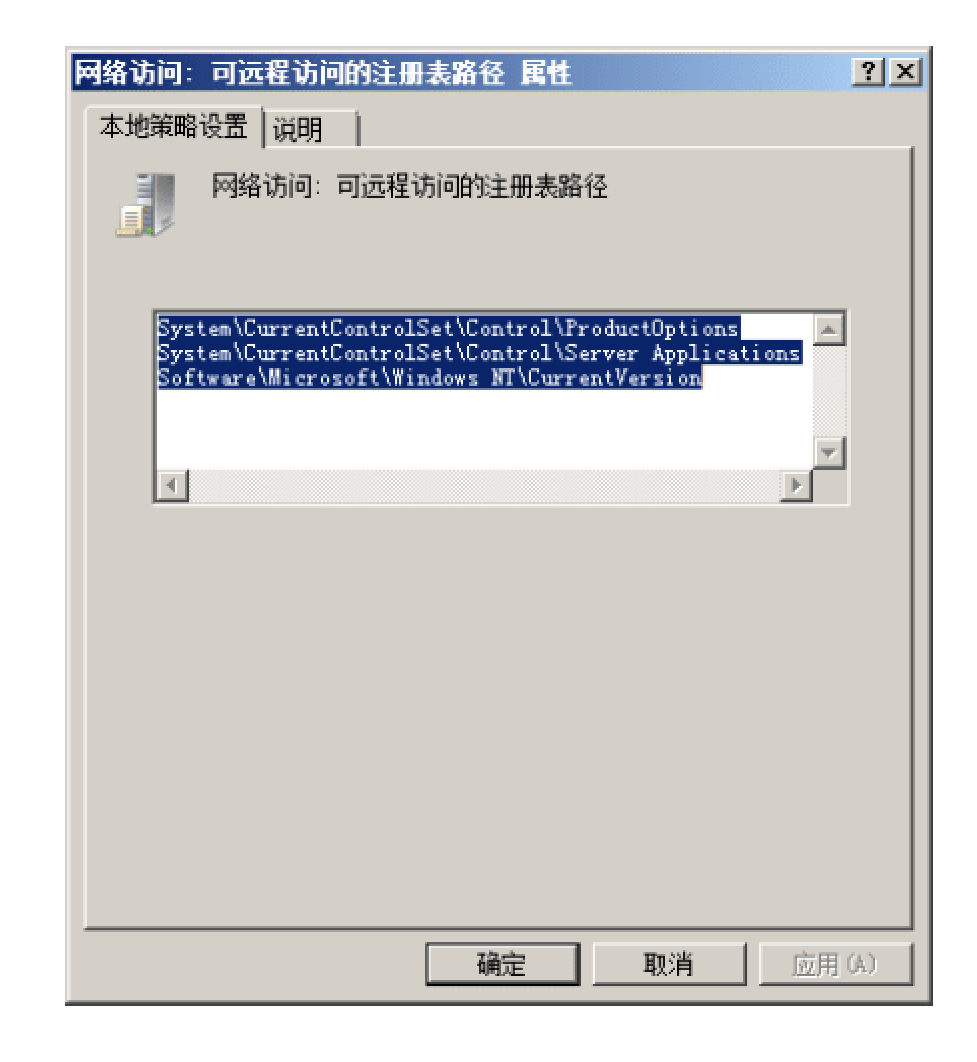


图 1-49　“网络访问：可远程访问的注册表路径 属性”对话框

2. 注册表安全设置

Windows Server 2008 系统注册表中常用的安全设置如下。

(1) 隐藏重要文件/目录可以修改注册表实现完全隐藏

找到如下注册表项：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
   Current-Version\Explorer\Advanced\Folder\Hi-dden\SHOWALL
```

右击 CheckedValue，选择快捷菜单中的“修改”命令，把数值由 1 改为 0。

(2) 对匿名连接的额外限制

没有显示的匿名权限就没有办法访问，在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
```

然后修改 restrictanonymous 为 2。

(3) 关闭默认的根目录和管理共享

去除 Windows 安装后生成的默认共享。在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters
```

添加 DWORD 值 autosharews 为 0，以及 autoshareserver 为 0。

(4) 禁止 Guest 用户访问日志

取消来宾账号机器同组账号访问日志的权利。在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog
```

将其 3 个子键 Application、Security、System 下面的 RestrictGuestAccess 值改为 1 即可。

(5) 禁止显示上次登录的用户名

防止在登录界面上泄漏账号信息。在注册表中找到

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
```

然后修改 Dontdisplaylastusername 为 1 即可。

(6) 禁用文件名创建

取消 Windows Server 2008 和 Windows Server 2003 为兼容以前微软文件名命名方式带来的性能损失。在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
```

然后设置 Ntfsdisable8dot3namecreation 为 1 即可。

(7) 禁用无用的子系统

取消因为使用例如 DOS、Win16、OS/2、Posix 应用系统下的程序子系统可能带来的隐患。

在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Subsystems
```

然后将 Optional 的值修改为“0000”。

删除同一子键下的 OS2、posix 项，同时找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\wow
```

删除其下的子键。

在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\ environment
```

然后删除其下的 OS2libpath 项。

在注册表中找到：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\os/2 Subsystem for nt
```

然后删除其下的所有子键。

(8) 不支持 IGMP 协议

在注册表中找到：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

然后新建 DWORD 值，改 IGMPLevel 值为 0 即可。

(9) 防止 ICMP 重定向报文的攻击

在注册表中找到：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

然后将 EnableICMPRedirects 值设为 0 即可。

(10) 修改终端服务端口

在注册表中找到：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
```

然后在右边的 PortNumber 键值下，在十进制状态下改成需要变更的端口号，只要不与其他端口冲突即可。

在注册表中找到：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Terminal Server\WinStations\RDP-Tcp
```

方法同上，记得端口号和上面改的一样就可以。

(11) 保护系统不受一定的拒绝服务攻击

要防备 SYN 泛滥攻击，在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\parameters
```

然后分别添加：

- DWORD 值 SynAttackprotect 为 2。
- Tcpmaxhalfopen 值为 100。
- Tcpmaxhalfopenedretried 的值为 80。
- Tcpmaxportsexhausted 的值为 5。

(12) 加强防备拒绝服务攻击

终止半开放的 TCP 连接，可在上面同一键下添加 Tcpmaxconnectreponseretransmissions 为 3。

(13) TCP 空连接计数器

可以防止死连接消耗资源，可以尽快结束死连接，在“7”的同一键值上面添加 DWORD 值 Keepalivetime 为 300000，该计算单位为毫秒，即 5 分钟。

(14) 不轻易改变 MTU 的值(最大传输单元)

防止 Windows Server 2008 和 Windows Server 2003 自动执行的 MTU 探索被恶意用户利用，导致系统采用极小 MTU 值从而增强资源消耗的拒绝服务攻击，可在同一键值下面添加 DWORD 值 Enablepmtudicovery 为 0。

(15) 禁用 IP 路由

防止恶意用户利用非法手段覆盖正常路由选择，应该在“7”的键值下面添加 DWORD 值 DisableIPsourcerouting 为 2。

(16) 禁用 ICMP 转向

防止恶意用户利用来改变 Windows Server 2008、Windows Server 2003 或路由表以响应网络设备发送给它的 ICMP 重定向消息，应该在“7”的键值下面修改 EnableICMPredirect 值为 0。

(17) 禁止光盘自动启动

防止恶意用户利用此手段访问系统，在注册表中找到：

```
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
```

然后设置 Nodrivetypeautorun 为 149。

(18) 只有本地用户才可以访问软盘

防止恶意用户利用此方法访问系统，在注册表中找到：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
```

然后修改 allocatefloppyes 值为 1。

(19) 只有本地登录的用户才能访问 CD-ROM

防止恶意用户利用此手段访问系统，修改同一键下的 allocatecdroms 值为 1。

(20) 在关机时清理虚拟内存页面交换文件

防止虚拟内存页面交换文件泄漏可用的信息，在注册表中找到：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Memory management
```

然后修改 clearpagefileatshutdown 值为 1。

1.4.4 审核策略

审核是 Windows Server 2008 系统中本地安全策略的一部分。通过设置审核策略，确定是否将安全事件记录到计算机上的安全日志中，同时也确定是否记录登录成功或登录失败，或二者都记录。安全日志是事件查看器的一部分。执行审核策略前，必须决定要审核的事件类别。为事件类别选择的审核设置将定义审核策略。



提示：在加入域中的成员服务器和工作站上，默认情况下未定义事件类别的审核设置。在域控制器上，默认情况下审核关闭。通过为特定的事件类别定义审核设置，可以创建一个适合组织安全需要的审核策略。

1. 审核策略的功能

安全事件日志一直都是令系统管理员头疼的问题。虽然通过分析安全事件可以从中发现许多实用信息，但是，由于数据量的巨大，需要耗费大量的时间和精力，很难快速从中得到有用的信息。

在 Windows Server 2008 中，审核系统有了很大的改进，管理员使用起来更加方便。审核策略的扩充，使用户可以更加方便的选择希望看到的事件。审核事件记录格式和内容也有所变化，使得用户能够更容易在安全日志中了解事件。另外，有关事件子系统及其相关工具的发展，解决了以往很多操作和分析的问题。

安全访问控制策略包括 3 项基本控制，即认证、授权和审核。认证是访问控制的“第一关”，负责验证对方身份的有效性，如用户名、密码等；授权是确认用户身份后，为其分配哪些访问权限，避免由于越界访问带来的安全隐患；审核则是记录用户访问过程中执行了哪些操作，是否对系统安全或网络安全构成威胁，并生成相应的日志。审核策略只能跟踪检查用户的操作是否违规，以及是如何违规的，但并不能防止违规事件的发生。

通过审核跟踪可以证明保护控制正在运行，随时检测审核跟踪来观察用户的活动是否违规。当系统发生意外后，管理员首先应从生成的日志中了解已发生的事情，在这种情况下，审核跟踪能够提供必要的证据。

2. Windows 审核的工作原理

Windows 审核系统、安全决策组件和事件日志服务配合工作，以可靠的方式为正在运行的网络服务生成安全事件。安全决策组件通常被称为安全参考监控，当制定了安全决策后，监视器就会通知审核系统，并将活动的细节传输到审核系统。审核系统将这些细节按照指定的格式生成事件日志，确保数据以连续形式显示，并且清除所有审核策略不允许日志的事件，其余事件被发送到事件日志服务，储存于安全日志中。图 1-50 中是 Windows 审核子系统的工作概况。

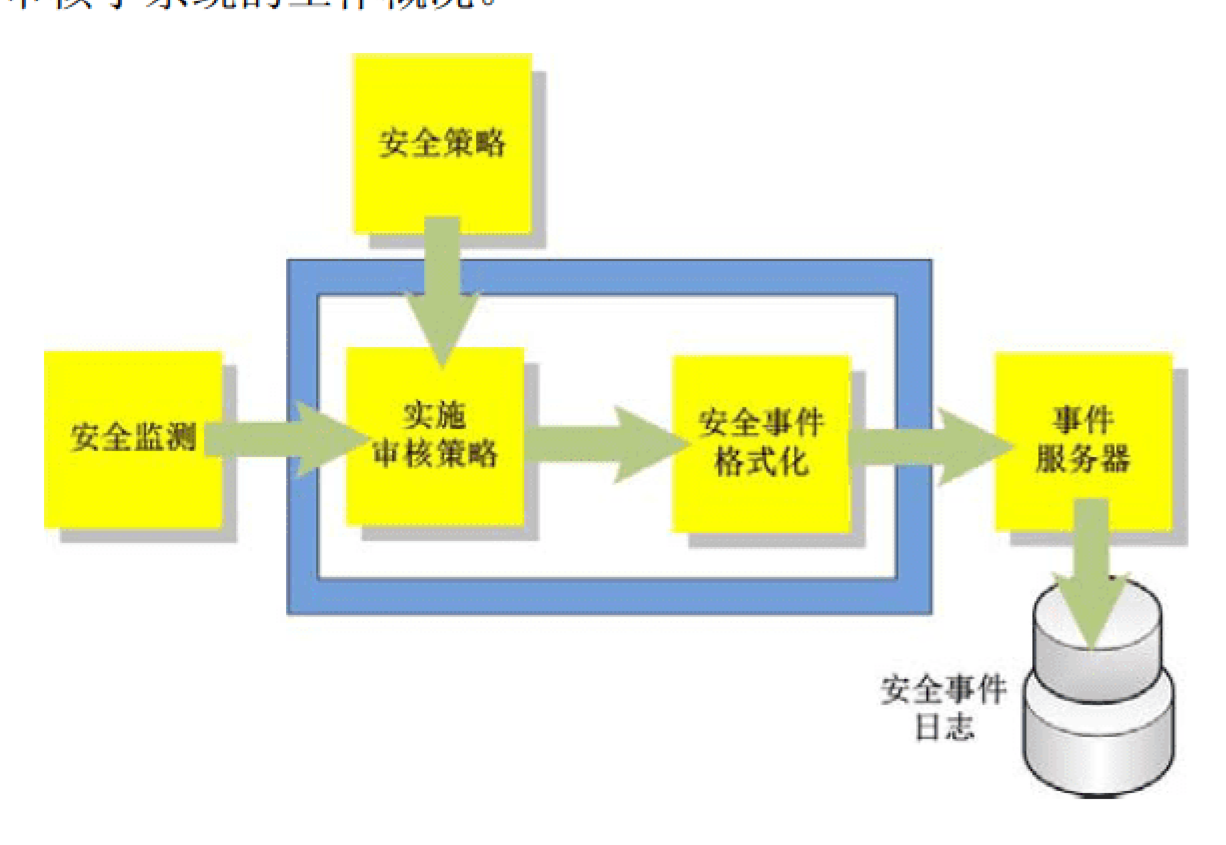


图 1-50　Windows 审核子系统

注意：Windows 审核在为审核系统提供事件前，会检查审核策略，预防发生不必要的执行障碍。

Windows 审核系统在 LSA 进程中执行，在 Windows 进程列表和 Windows 核心中显示为 lsass.exe。LSA 包含 Windows 用户模式组件，用于执行安全策略和其他安全功能，例如认证。有些组件(如认证包)是位于 LSA 内部的，将事件直接传递到审核系统。运行于 LSA 外的用户模式中的组件(如 ADDS)，以及使用 Windows 审核 APIs 的应用程序，只能经由 PRC 将事件传递到 LSA。内核包含着一个普通的审核界面供核心组件使用。它还包含一个对象管理器，负责生成多数对象访问事件。事件可以通过内核事件跟踪引擎(ETW)传递到事件日志服务，也可以通过 RPC 传递。大多数生成于内核的事件直接传递到 ETW，但复杂的事件则需先传递到 LSA 进行格式化。LSA 将多数事件通过 ETW 传递到事件日志，只有在部分审核子系统失败时才使用 RPC 渠道。



提示：在 Windows Vista 和 Windows Server 2008 系统中，事件日志引擎已经升级到 6.0 版本。旧的事件日志服务最大的有效日志文件为 4GB(在 x86 的计算机上会更小些)，而使用新版本引擎的日志文件可以超过一个 PB。旧日志的最大传输速率为每秒几千个事件，而新日志的传输速率为每秒上万个。

3. 系统审核类型

(1) 审核账户登录事件

审核账户登录事件设置确定是否审核在这台计算机用于验证账户时，用户登录到其他计算机或者从其他计算机注销的每个实例。当在域控制器上对域用户账户进行身份验证时，将产生账户登录事件。该事件记录在域控制器的安全日志中。当在本地计算机上对本地用户进行身份验证时，将产生登录事件。该事件记录在本地安全日志中，不产生账户注销事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。当某个账户的登录成功时，成功审核会生成审核项。当某个账户的登录失败时，失败审核会生成审核项。

(2) 审核账户管理

审核账户管理设置确定是否审核计算机上的每一个账户管理事件。账户管理事件的例子包括：

- 创建、更改或删除用户账户或组。
- 重命名、禁用或启用用户账户。
- 设置或更改密码。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。任何账户管理事件成功时，成功审核都会生成审核项。任何账户管理事件失败时，失败审核都会生成审核项。

(3) 审核目录服务访问

审核目录服务访问设置确定是否审核用户访问那些指定自己的系统访问控制列表(SACL)的 Active Directory 对象的事件。

默认情况下，在“默认域控制器组策略对象(GPO)”中该值设置为无审核，并且在该值没有任何意义的工作站和服务器中，它保持未定义状态。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。用户成功访问指定了 SACL 的 Active Directory 对象时，成功审核会生成审核项。用户尝试访问指定了 SACL 的 Active Directory 对象失败时，失败审核会生成审核项。



注意：通过使用某个 Active Directory 对象“属性”对话框中的“安全”选项卡，可以设置该对象的 SACL。该操作与审核对象访问相同，只不过它仅应用于 Active Directory 对象而不是文件系统和注册表对象。

(4) 审核登录事件

审核登录事件设置确定是否审核每一个登录或注销计算机的用户实例。

在域控制器上将生成域账户活动的账户登录事件，并在本地计算机上生成本地账户活动的账户登录事件。如果同时启用账户登录和账户审核策略类别，那么使用域账户的登录将生成登录或注销工作站或服务器的事件，而且将在域控制器上生成一个账户登录事件。此外，在用户登录而检索登录脚本和策略时，使用域账户的成员服务器或工作站的交互式登录将在域控制器上生成登录事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。登录成功时，成功审核会生成审核项。登录失败时，失败审核会生成审核项。

(5) 审核对象访问

审核对象访问设置确定是否审核用户访问某个对象的事件，例如文件、文件夹、注册表项、打印机等，它们都有自己特定的系统访问控制列表(SACL)。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。当用户成功访问指定了合适 SACL 的对象时，成功审核将生成审核项。当用户访问指定有 SACL 的对象失败时，失败审核会生成审核项。

(6) 审核策略更改

审核策略更改设置确定是否审核用户权限分配策略、审核策略或信任策略更改的每一个事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。对用户权限分配策略、审核策略或信任策略所作更改成功时，成功审核会生成审核项。对用户权限分配策略、审核策略或信任策略所作更改失败时，失败审核会生成审核项。

(7) 审核特权使用

审核特权使用设置确定是否审核用户实施其用户权利的每一个实例。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对这种事件类型进行审核。用户权利实施成功时，成功审核会生成审核项。用户权利实施失败时，失败审核会生成审核项。

(8) 审核过程跟踪

审核过程跟踪设置确定是否审核事件(例如程序激活、进程退出、句柄复制和间接对象访问等)的详细跟踪信息。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。所跟踪的过程成功时，成功审核会生成审核项。所跟踪的过程失败时，失败审核会生成审核项。

(9) 审核系统事件

当用户重新启动或关闭计算机时或者对系统安全或安全日志有影响的事件发生时，安全设置确定是否予以审核。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。系统事件执行成功时，成功审核会生成审核项。系统事件执行失败时，失败审核会生成审核项。

第 2 章　Windows Server 2008 系统加固

任何安全措施都无法确保万无一失，强有力的安全措施可以增加入侵难度，从一定程度上提升系统安全性。通常情况下，用户安装操作系统后，只是进行简单的安全设置，便投入应用，其实这是非常危险的。要想使服务器在复杂的网络环境中平稳运行，必需从各方面实施安全加固，包括安装系统更新、账户安全、访问权限控制和系统服务安全等。

关键词

- 安装系统更新
- 系统管理员账户
- 磁盘访问权限
- 系统账户数据库
- 系统服务安全
- 端口安全
- 系统漏洞安全

2.1　安装系统更新

配置适当的系统更新方式，可以确保在第一时间获取软件公司发布的各种系统更新，但是这些更新程序并非适用于所有系统环境，安装更新时应注意其运行环境和主要功能。如果条件允许，建议大规模部署之前，在实验环境中进行测试，以免在安装更新程序后，导致网络服务或其他应用程序无法正常运行。

2.1.1　补丁安装注意事项

Windows 系统补丁程序都是由微软网站发布的，用于弥补相应操作系统漏洞或缺陷。通常情况下，有手动安装和自动安装两种方式。手动安装补丁程序多用于不支持自动下载和安装更新内容的 Windows 操作系统，或者不方便在线获取更新内容的安装。手动安装补丁程序与普通应用程序的安装比较相似。补丁程序可以通过登录相关网站直接下载，也可以购买含有补丁程序的安装光盘。

在安装系统更新时，应该注意以下问题：

- 机器在没有安装补丁之前切记不要联网。所需的补丁程序在其他计算机下载后，使用其移动存储设备或者刻录成光盘，复制到需要安装补丁的服务器。
- 某些补丁程序对安装顺序有要求，否则无法完成安装或导致安装失败。
- 开始安装补丁程序前应首先关闭其他应用程序，以免导致安装失败。另外，有些补丁程序安装完成后需要重新启动计算机方可生效，打开的应用程序应注意及时保存当前的结果。
- 获取补丁程序时应注意其版本要求，不仅要注意操作系统的类型，还应注意英文版和简体中文版、繁体中文版的区别。
- 安装过程中如需确认或更改安装目录的，建议保持系统默认设置。

2.1.2　补丁安装

如果用户选择了“计划安装”方式，则安装向导将自动下载并安装系统更新，只是在必要时会提示重新启动计算机。

① 依次单击“开始”→“Windows Update”，显示如图 2-1 所示的 Windows Update 窗口，提示更新的数量和大小。

② 单击“查看可用更新”链接，显示如图 2-2 所示的“查看可用更新”窗口，不需要的更新可以直接取消选中其前面的复选框。如果不希望系统再次提示安装取消的更新，则右击该更新并选择快捷菜单中的“隐藏”命令即可。

③ 单击“安装”按钮，或者在 Windows Update 窗口中单击“安装更新”按钮，显示如图 2-3 所示的窗口，开始下载并安装指定更新(与管理员设置的更新方式有关)。



图 2-1　Windows Update 窗口

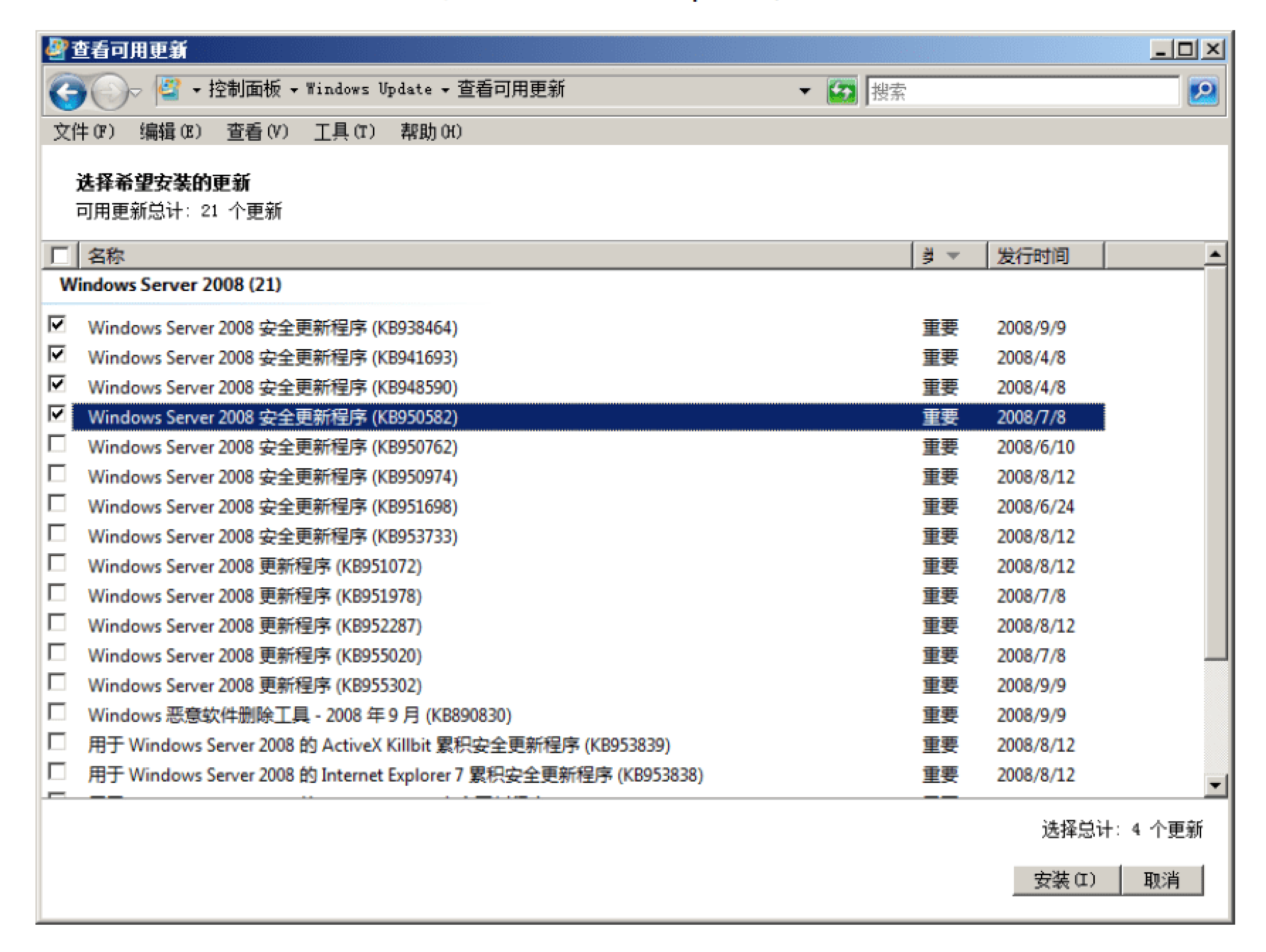


图 2-2　“查看可用更新”窗口

④　安装完成后，显示如图 2-4 所示的窗口，安装结果中包括安装成功或失败的数量，以及是否需要重新启动计算机。如果安装的更新涉及的应用程序正在运行，则可能导致安装失败。



图 2-3 正在下载和安装



图 2-4 安装完成

⑤ 某些更新必须在重新启动系统后方可生效，此时，可以单击“立即重新启动”按钮重启计算机，也可以稍后再重新启动。系统默认等待 10 分钟后自动显示如图 2-5 所示的对话框。可在“请在以下时间段之后提醒我”下拉列表中选择等待的时间，如 10 分钟、1 小时、4 小时等。

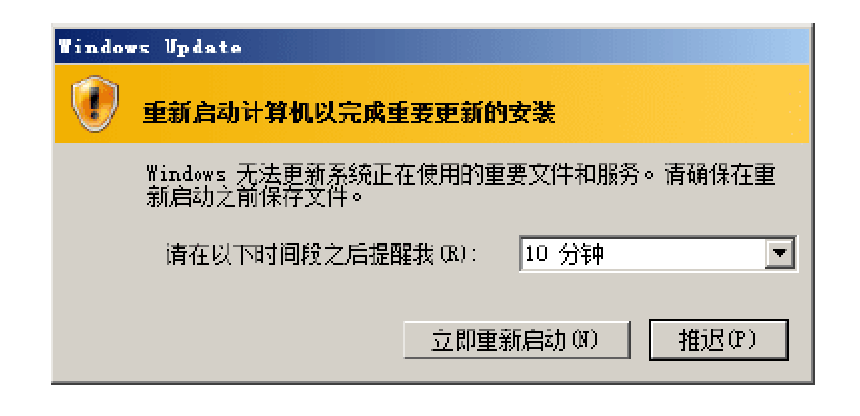


图 2-5 Windows Update 对话框

⑥ 单击“推迟”按钮，即可在指定时间后再次收到该提示信息，根据实际情况选择立即重新启动或者继续推迟即可。

2.2　系统管理员账户

系统管理员账户是 Windows 系统中权限最高的用户账户，一旦被入侵者破解或丢失，后果将不堪设想。因此，必须做好系统管理员账户的安全保护工作，如更改账户名称、设置密码、创建陷阱账号等。

2.2.1　更改 Administrator 账户名称

安装 Windows Server 2008 系统后，默认会自动创建一个系统管理员账户，即 Administrator。许多系统管理员贪图一时方便，就直接用作自己的账户，因此，许多黑客攻击服务器时总是试图破解 Administrator 账户的密码，如果此时密码安全性不高，后果可想而知。通常情况下，可以通过更改管理员账户名称来避免此类攻击，提高系统安全性。

1. 更改本地计算机 Administrator 账户名

以 Administrator 账户登录本地计算机，依次单击“开始”→“管理工具”→“计算机管理”，打开“计算机管理”窗口，展开“系统工具”→“本地用户和组”→“用户”，右击 Administrator 账户并选择“重命名”，并输入新的账户名称即可，如图 2-6 所示。设计新的账户名称即可，尽量不要使用 Admin、master、guanliyuan 之类的名称，否则账户安全性同样没有任何保障。

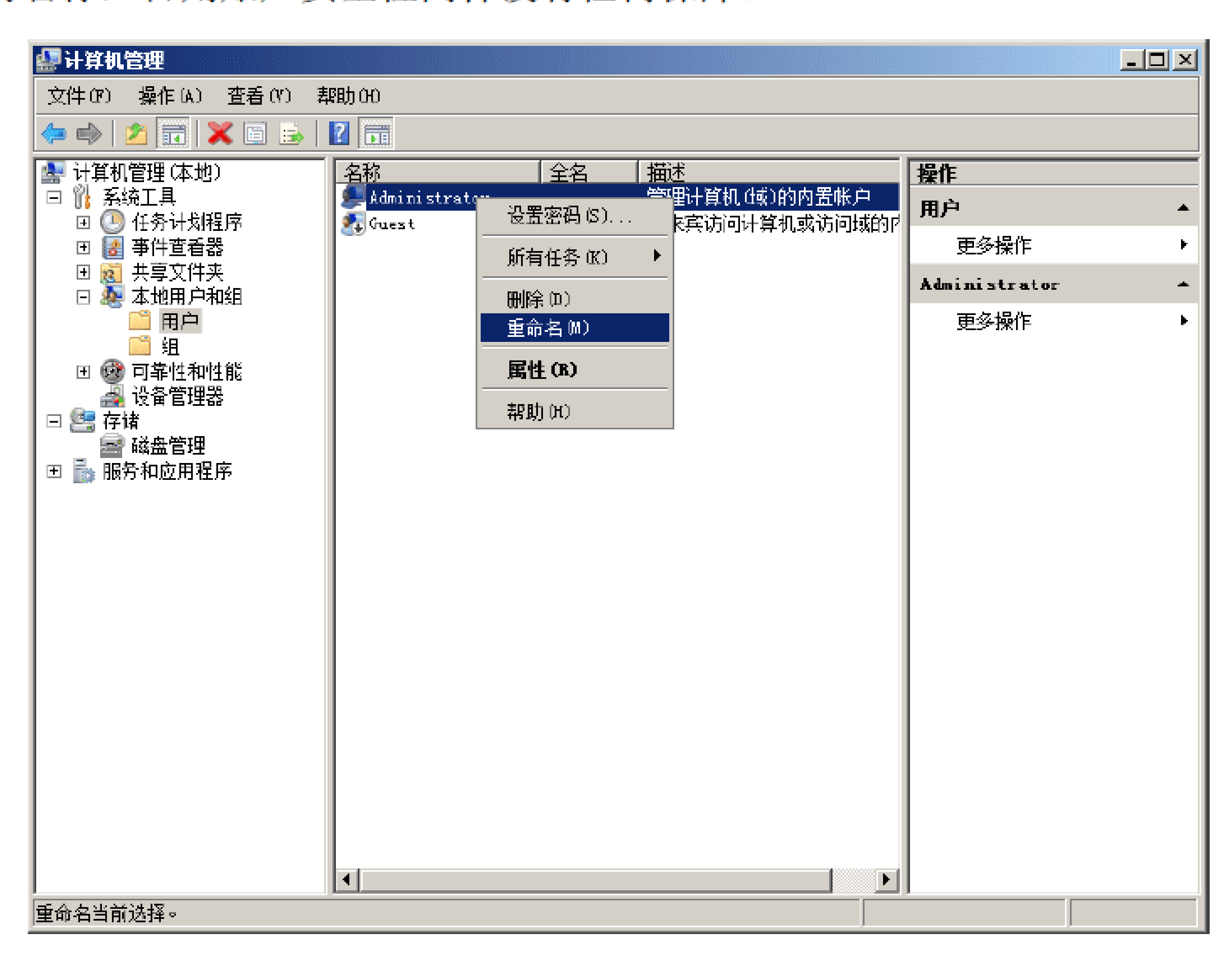


图 2-6　“计算机管理”窗口

2. 更改域 Administrator 账户名

域中的所有用户账户默认都是存放在域控制器的 Users 容器中的，Administrator 账户是整个域的超级管理员用户。依次单击“开始”→“管理工具”→“Active Directory 用户和计算机”，打开如图 2-7 所示

的“Active Directory 用户和计算机”窗口，在 Users 容器中右击 Administrator 账户，并选择快捷菜单中的“重命名”命令即可。

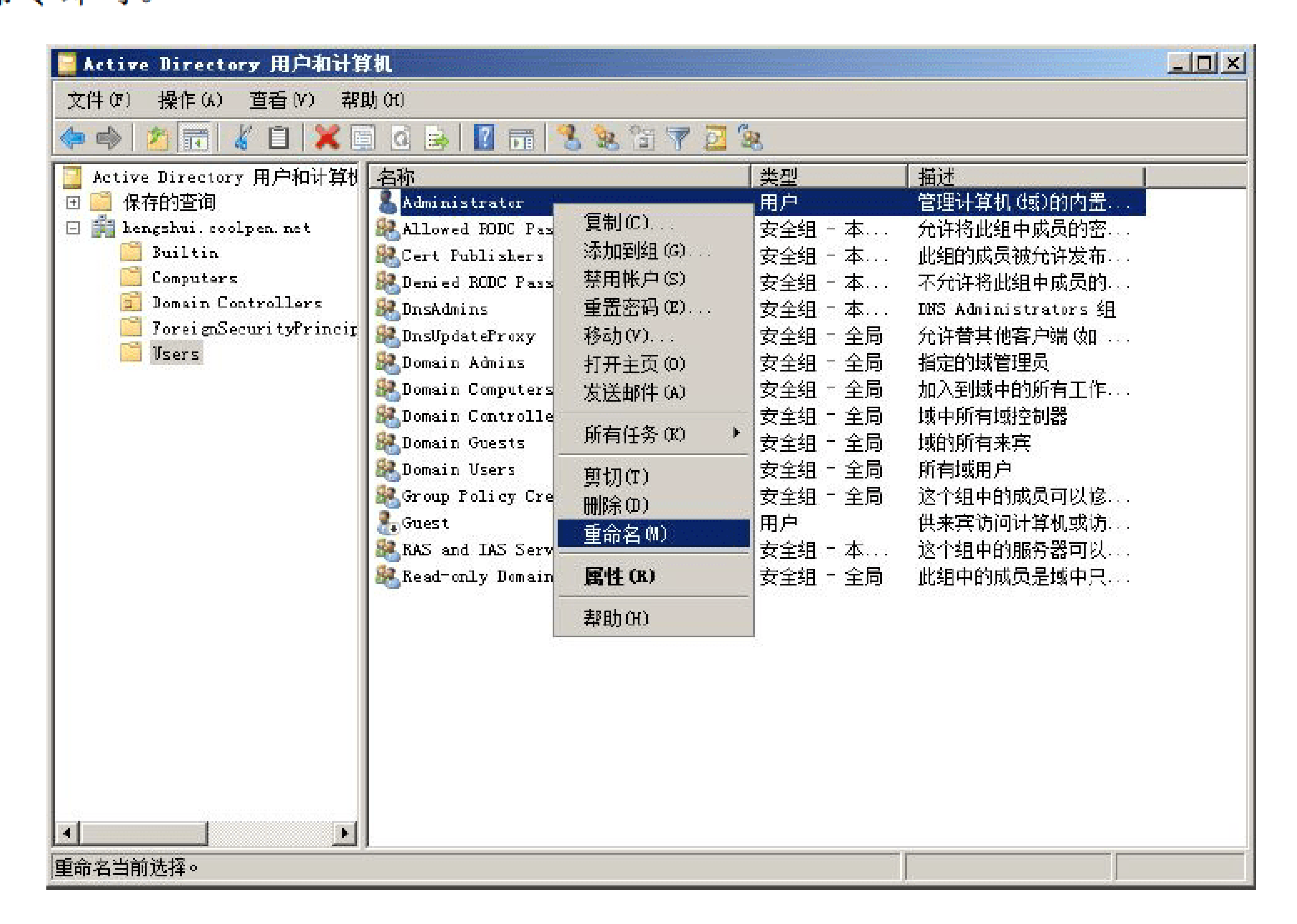


图 2-7 “Active Directory 用户和计算机”窗口

输入新的账户名并确认时，会显示如图 2-8 所示的“Active Directory 域服务”对话框，建议更改之后立即注销并使用新的账户名登录，以避免出现访问冲突。单击“是”按钮，关闭该对话框，稍后注销当前用户账户即可。

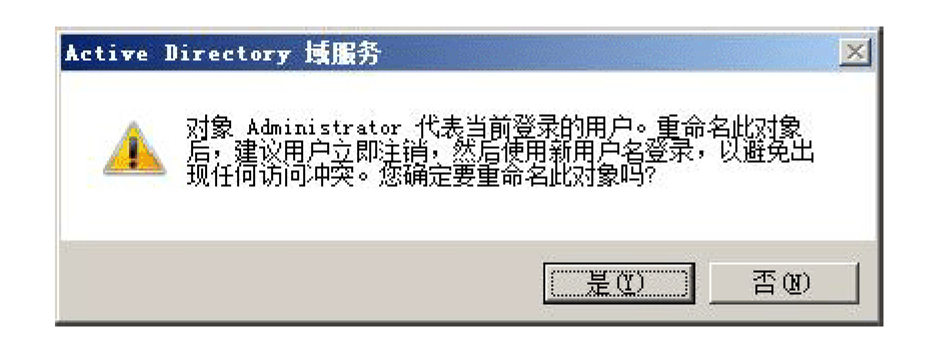


图 2-8 “Active Directory 域服务”对话框

3. 通过组策略更改 Administrator 账户名

无论是独立计算机还是域控制器，都可以通过 Windows 组策略更改 Administrator 账户名称。如果是独立计算机，则可以依次单击“开始”→“管理工具”→“本地安全策略”，打开“本地安全策略”控制台；依次展开“安全设置”→“本地策略”→“安全选项”，在右侧主窗口中双击“账户： 重命名系统管理员账户”，打开“账户：重命名系统管理员账户 属性”对话框，如图 2-9 所示。重新输入新的账户名称即可。

如果是域控制器，则需要依次单击“开始”→“管理工具”→“组策略管理”，找到作用于根域的默认策略 Default Domain Policy，右击并选择快捷菜单中的“编辑”，打开“组策略管理编辑器”窗口，依次展开“策略”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，双击右侧主窗口中的“账户： 重命名系统管理员账户”，打开“账户：重命名系统管理员账户 属性”对话框，系统默认是没有定义该策略的，选中“定义这个策略设置”复选框，并在文本框中输入新的名称即可，如图 2-10 所示。

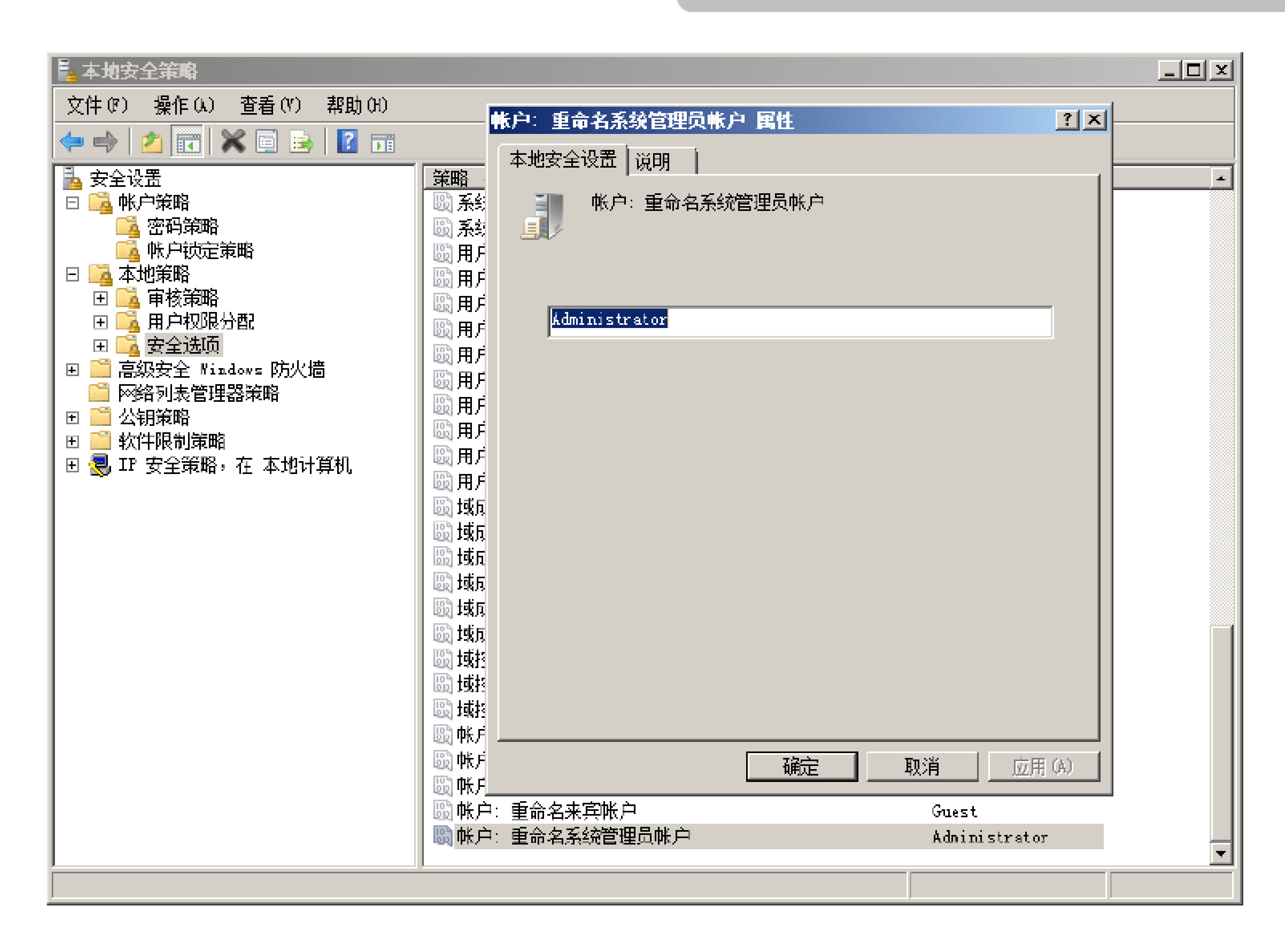


图 2-9　通过本地安全策略更改管理员账户名

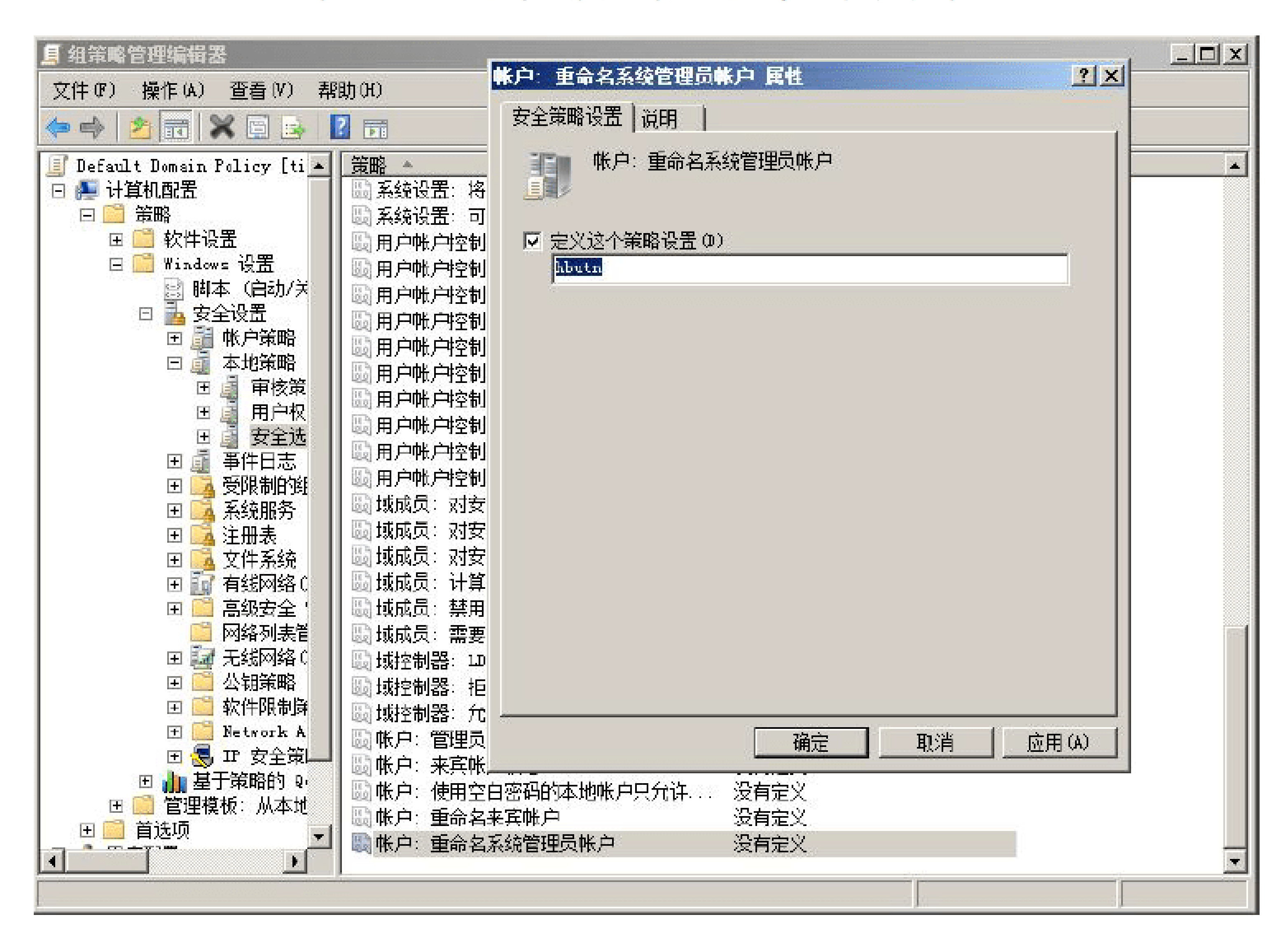


图 2-10　通过域安全策略更改管理员账户名

2.2.2　禁用 Administrator 账户

如果更改账户名仍无法满足安全需求，可以选择直接将其禁用，然后创建一个普通的管理员账户，用于实现基本的系统或者网络管理、维护功能。如此一来，再高明的黑客也将无法获取超级管理员账户权限。

在“计算机管理”控制台的“本地用户账户和组”→“用户”窗口中，双击 Administrator 打开如图 2-11 所示的“Administrator 属性”对话框。选中“账户已禁用”复选框即可。如果是 Windows 域控制器，则可以在“Active Directory 用户和计算机”的 Users 容器中，进行此项设置。

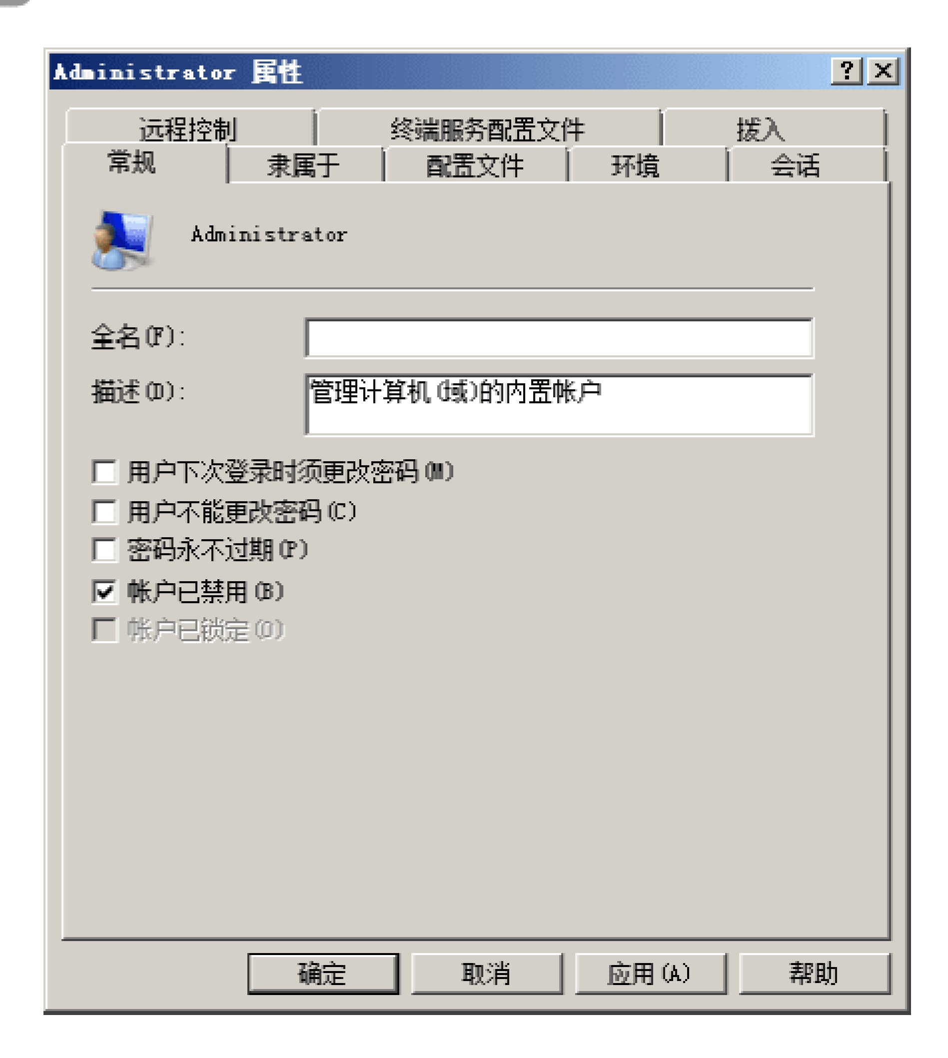
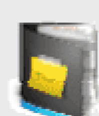


图 2-11 “Administrator 属性”对话框

禁用 Administrator 账户相对于为其更名而言，安全性更高。但是，当需要完成某些特殊管理任务而用到超级管理员账户时，必须先进入安全模式，重新启用该账户，如进行目录恢复和还原等。



提示：用户自定义的管理员，虽然同样属于某些系统管理员组，但却无法获得超级管理员的权限，功能方面仍有很大区别。

2.2.3 减少管理员组成员

尽量减少管理员组成员的数量，也是最大限度保证网络安全的重要措施。对于独立计算机而言，可以在“计算机管理”→“本地用户和组”→“组”中，双击 Administrators 打开如图 2-12 所示的“Administrators 属性”对话框，选择“成员”列表中想要删除的管理员账户，并单击“删除”按钮即可。

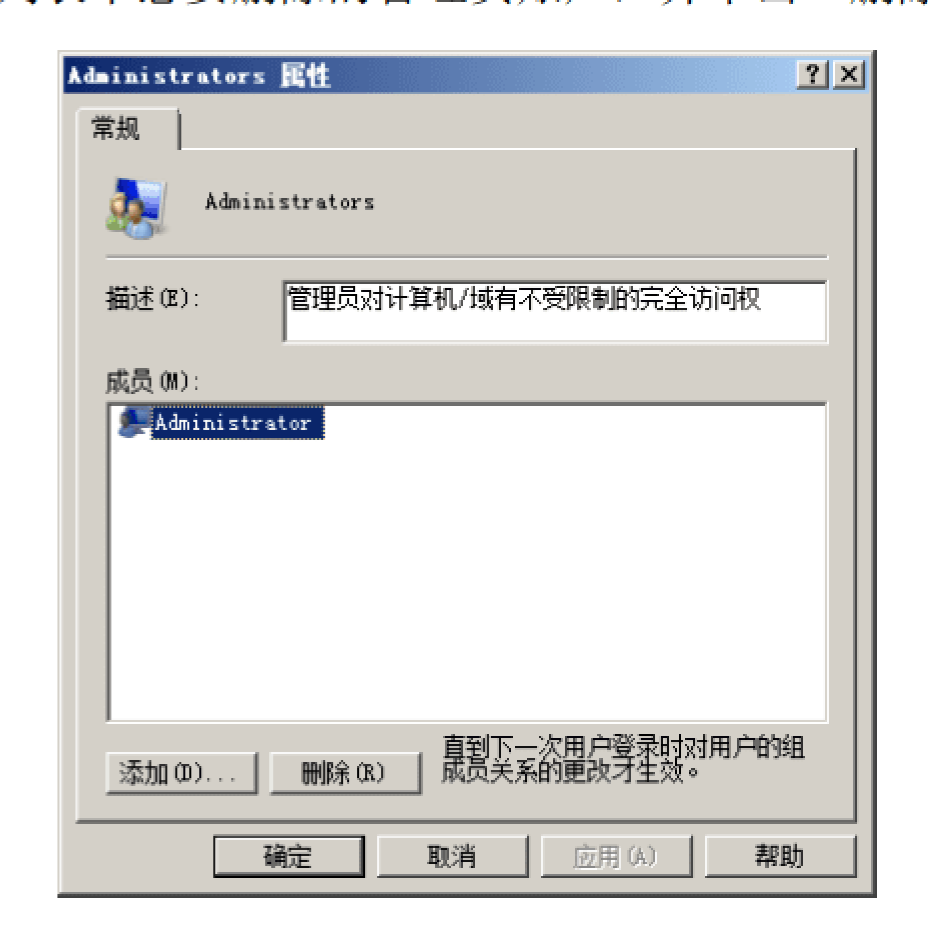


图 2-12 “Administrators 属性”对话框

如果是域控制器，则除减少 Administrators 组中的成员之外，还应严格控制添加到 DnsAdmins 组和 Enterprise Admins 组中的成员账户，这些组同样是 Administrators 组中的成员。管理员账户的数量越少，密码丢失或被破解的可能性就越小，系统也就越安全。

2.2.4 系统管理员口令设置

入侵者若想盗取系统内的重要数据信息或执行某项管理功能，就必须先获得管理员权限，即破解管理员账户密码。密码破解软件工作机制主要包括 3 种：巧妙猜测、词典攻击和自动尝试字符组合。从理论上讲，只要有足够时间，使用这些方法可以破解任何账户密码，破解一个弱密码可能只需几秒钟即可完成，而要破解一个安全性较高的强密码则可能需要几个月甚至几年的时间。因此，系统管理员账户必须使用强密码，并且要经常更改密码。

1. 注意事项

在设置管理员账户密码时，应注意以下问题。

(1) 切不可让账号与密码相同

如果将用户账号与密码设置为相同，许多系统扫描工具默认将账户和密码作为相同的设置扫描系统，无疑会省去攻击者的很多力气。

(2) 切不可使用自己的姓名

使用自己的姓或名、甚至是姓名作为密码，实在是不堪一击，对于本单位和熟悉本单位的人来讲，姓名无疑是攻击的首选，因为这几乎谁都能猜得到。另外，在许多黑客编写的字典中，往往将百家姓一一列出，并放在字典的前列。

(3) 切不可使用英文词组

一些常用或别致的英文单词往往是用户设置密码时的最爱，在他们看来，这类密码既便于记忆，又凸显自己的个性。但事实上，那些绝顶聪明的黑客们也早已猜到并详细地将其编入字典，因此，英文词组绝不可用。

(4) 切不可使用特定意义的日期

以具有特定意义的日期作为密码是任何人都十分喜爱的，这一类日期通常有自己生日、父母生日、儿女生日、朋友生日、重大节日、个人纪念日等。不用说熟悉的人可以猜得到，即使是陌生人也可以通过穷举的方式而得手。

(5) 切不可使用简单的密码

越是字符数少则越是简单的密码，在破解时所用的时间也就越短。一个以穷举软件每秒钟可以重试 10 万次之多，字数越少，字符越简单化，排列组合的结果也就越少，也就越容易被攻破。

2. 安全密码原则

若欲保证账户密码的安全，应当遵循以下规则：

- 用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符，将这些符号排列组合使用，以期达到最好的保密效果。
- 用户密码不要太规则，不要将用户姓名、生日和电话号码作为密码。不要用常用单词作为密码。
- 根据黑客软件的工作原理，参照密码破译的难易程度，以破解需要的时间为排序指标，密码长度

设置时应遵循 7 位或 14 位的整数倍原则。

- 在通过网络验证密码过程中，不得以明文方式传输，以免被监听截取。
- 密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上并且包含密码的文件是只读的。加密的方法很多，如基于单向函数的密码加密，基于测试模式的密码加密，基于公钥加密方案的密码加密，基于平方剩余的密码加密，基于多项式共享的密码加密，基于数字签名方案的密码加密等。经过上述方法加密的密码，即使是系统管理员也难以得到。
- 密码应定期修改，应避免重复使用旧密码，应采用多套密码的命名规则。
- 建立账号锁定机制。一旦同一账号密码校验错误若干次即断开连接并锁定该账号，经过一段时间才解锁。
- 由网络管理员设置一次性密码机制，用户在下次登录时必须更换新的密码。

3. 系统账户密码要求

在 Windows Server 2008 系统中，安装系统的同时就要求管理员必须指定符合要求的安全密码，大大提高了用户账户和系统的安全性。通常情况下，Windows Server 2008 网络中，对用户账户密码要求如下：

- 不包含全部或部分的用户账户名。
- 长度至少为 6 个字符。
- 包含来自以下 4 个类别中的 3 个的字符：
  - 大写英文字母(从 A～Z)。
  - 小写英文字母(从 a～z)。
  - 10 个基本数字(从 0～9)。
  - 非字母字符(例如，!、$、#、%)。

对于未安装 Active Directory 服务 Windows Server 2003 计算机或修改了 Windows Server 2003/2008 默认组策略的计算机，其用户账户密码可以随意设置。

强密码具有以下特征：

- 长度至少有 7 个字符。
- 不包含用户的生日、电话、用户名、真实姓名或公司名等。
- 不包含完整的字典词汇。
- 包含全部下列 4 组字符类型。大写字母(A,B,C...)、小写字母(a,b,c...)、数字(从 0～ 9)、非字母字符(键盘上所有未定义为字母和数字的字符，如` ～ !@#$%^&*()_+-={}|[]\:";'<>?,/)。

除此之外，管理员账户的密码应当定期修改，尤其是当发现有不良攻击时，更应及时修改复杂密码，以避免被破解。为避免密码因过于复杂而忘记，可用笔记录下来，并保存在安全的地方，或随身携带避免丢失。其实，最安全的方法就是不使用常规密码，而采用电子密钥等一些几乎无法破解的登录方式，确保系统安全性。

2.2.5 创建陷阱账户

所谓陷阱账户就是名称与默认管理员账户名称(Administrator)类似或完全相同，而权限却极低的用户账户。这种方法通常和“更改 Administrator 账户名称”配合使用，即将系统管理员账户更名后，再创建一个名称为 Administrator 的陷阱账户。

① 创建一个名称为 Administrator 的用户账户(如果原有管理员账户没有被更名则可以创建一个名称类似的账户，如 Admin 等)，并输入一个复杂程度极高的安全密码，选中“密码永不过期”复选框，如图 2-13 所示。

② 单击“创建”按钮即可创建该账户。

③ 将其从 Users 组中删除，这样就可以避免其集成来自 Users 组的用户权限，如图 2-14 所示。选择陷阱账户 Administrator 并单击“删除”按钮，将其删除。最后单击“确定”按钮保存。



图 2-13　创建陷阱账户

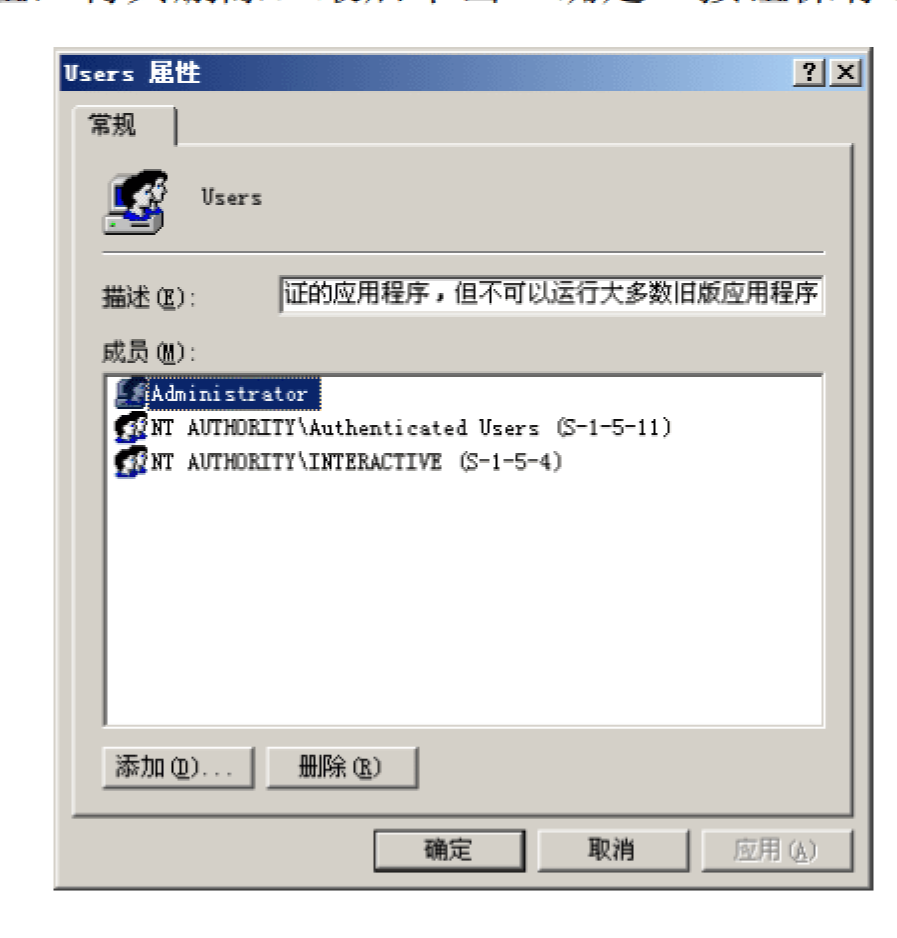


图 2-14　删除 Users 组中的陷阱账户

④ 双击陷阱账户，打开用户账户属性对话框，将其各种权限设置为最低。例如，在“拨入”选项卡中，“网络访问权限”选项区域中选择“拒绝访问”单选按钮，如图 2-15 所示。

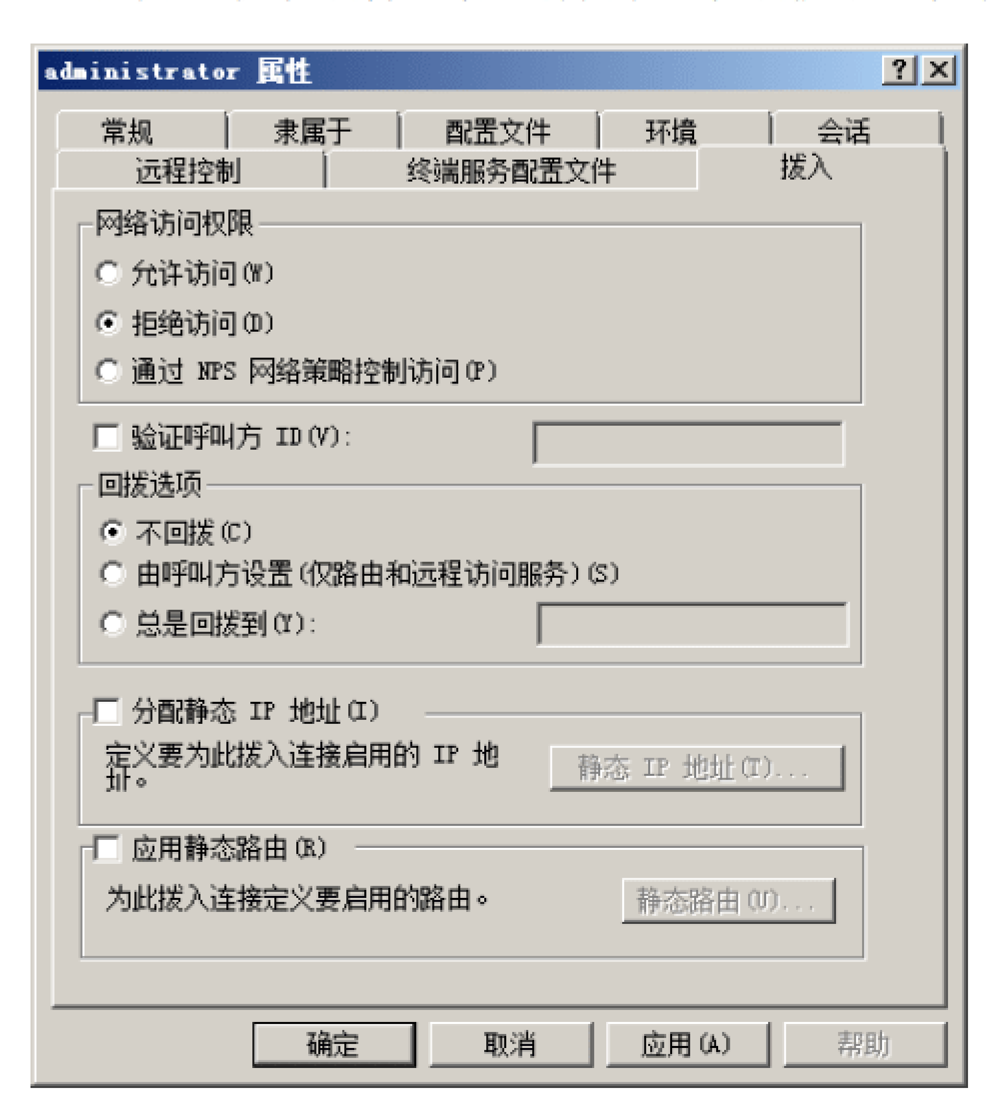


图 2-15　限制陷阱账户的权限

⑤ 单击“确定”按钮保存设置。



注意：除此之外，还可以在所有磁盘分区的 NTFS 权限列表中一一删除陷阱账户的各种权限。总之，使其不具备任何操作权限，即使被盗用也无法进行任何破坏操作。

2.3　磁盘访问权限

权限有高低之分，具备高权限的用户可以访问、修改低权限用户的文件夹和文件。除了 Administrators 之外，其他组的用户不能访问 NTFS 卷上的其他用户资料。除非获得了显式授权，具备低权限的用户无法访问、修改具备高权限用户的文件夹和文件。

2.3.1　权限范围

Windows Server 2008 操作系统对 NTFS 卷及其包含的目录或者文件提供了权限设置，分别是完全控制、修改、读取和运行、列出文件夹目录、读取、写入和特殊的权限。下面简要介绍这 7 种权限的控制范围。

- 完全控制：拥有不受限制的完全访问。地位就像 Administrators 在所有组中的地位一样。选中“完全控制”复选框，其他的 5 项属性(修改、读取和运行、列出文件夹目录、读取、写入)将自动被选中。
- 修改：选中了“修改”复选框，其他的 4 项属性(读取和运行、列出文件夹目录、读取、写入)将自动被选中。如果 4 项属性账户的任何一项没有被选中，“修改”条件将不再成立。
- 读取和运行：允许读取和运行卷、目录或者文件下的任何文件，“列出文件夹目录”和“读取”是“读取和运行”的必要条件。
- 列出文件夹目录：只能浏览卷、目录或者文件下的子目录，不能读取，也不能运行(NTFS 卷上的文件权限范围中不包含此项)。
- 读取：能够读取卷、目录或者文件下的数据。
- 写入：可以向卷、目录或者文件下写入数据。
- 特殊的权限：对以上的 6 种权限进行了细分。读者可以根据需要对“特别的权限”进行深入的设置。

Windows Server 2008 操作系统安装完成后，对系统磁盘 C 的权限默认设置如图 2-16 所示。

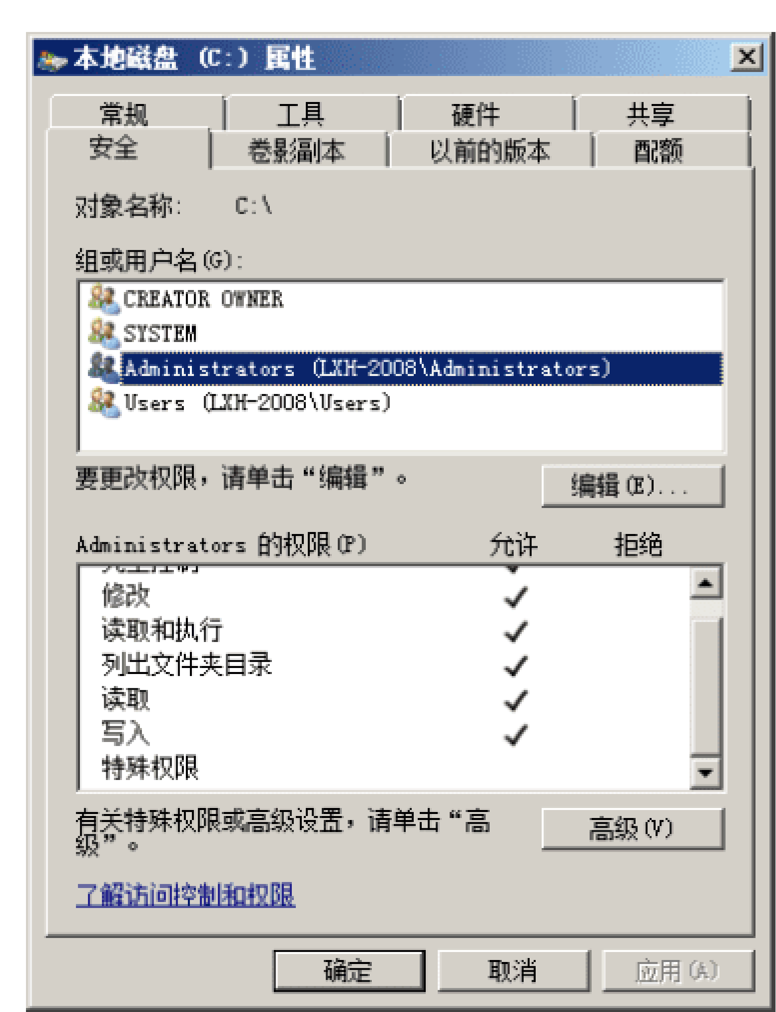


图 2-16　系统磁盘的默认设置

建议对默认系统磁盘权限设置进行如下修改：

- 系统盘及所有磁盘只赋予 Administrators 组和 SYSTEM 组的完全控制权限。
- 系统盘“\用户”目录只赋予 Administrators 组和 SYSTEM 组的完全控制权限。
- 系统盘\Windows\System32\cacls.exe、cmd.exe、net.exe、ftp.exe、tftp.exe、telnet.exe、netstat.exe、regedit.exe、at.exe、attrib.exe、format.com、del 文件只给 Administrators 和 SYSTEM 的完全控制权限，将\System32\cmd.exe、format.com、ftp.exe

转移到其他目录或更名。

- 用户账户对应文件夹中的文件和文件夹仅赋予所属用户和 Administrators 完全控制权限。

2.3.2　设置磁盘访问权限

默认情况下，安装完成 Windows Server 2008 后，系统自动赋予某些用户账户和组部分权限。为了确保系统安全，建议系统管理员对默认的磁盘权限进行调整，仅授予 Administrators 和 SYSTEM 才可以访问的权限即可。

① 打开“我的计算机”窗口，显示当前系统安装的所有系统磁盘。右击“本地磁盘(C:)”图标，在弹出的快捷菜单中选择“属性”命令，打开“本地磁盘(C:)属性”对话框。切换到“安全”选项卡，选择相应的“组或用户名”，单击“编辑”按钮，即可编辑希望赋予权限的用户或组，如图 2-17 所示。

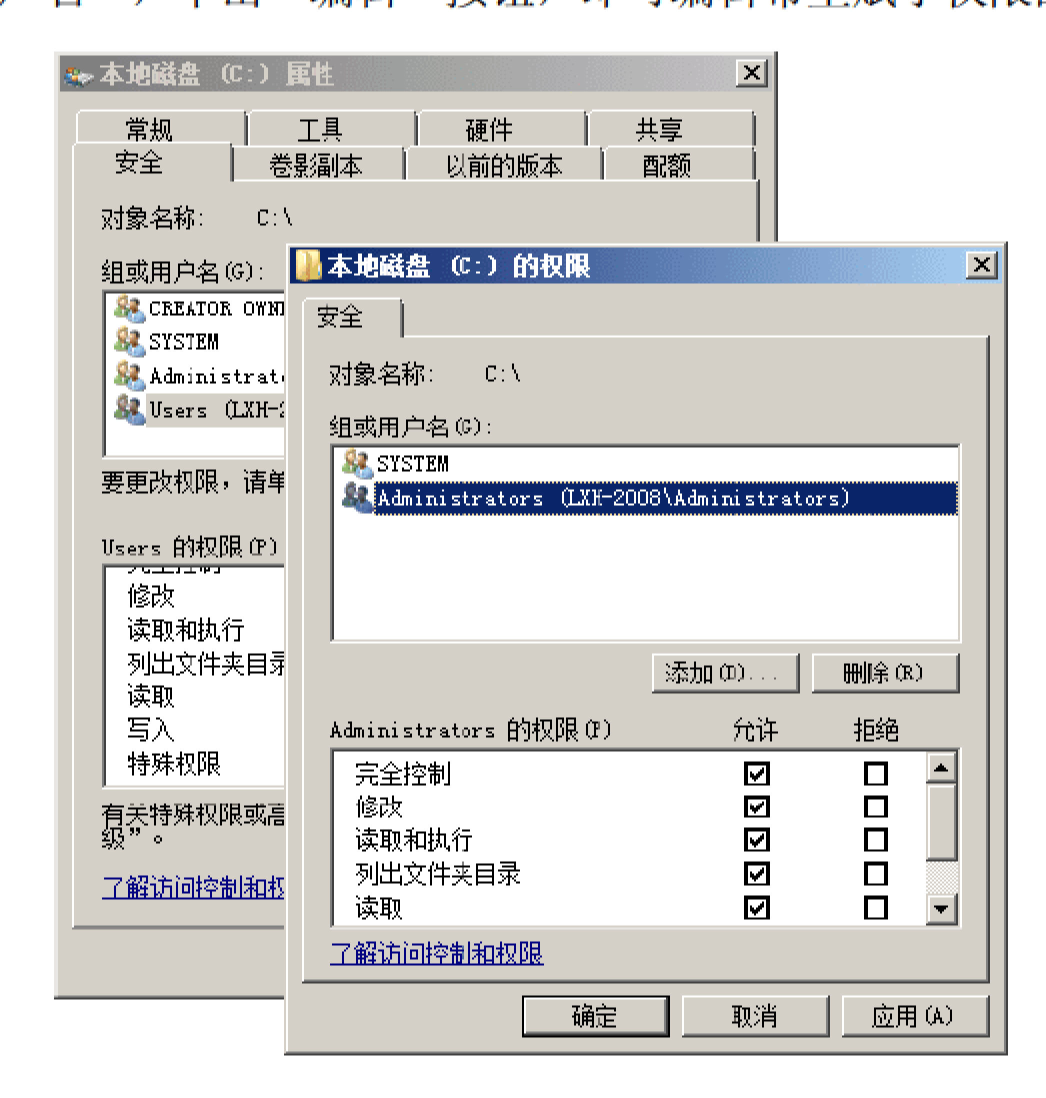


图 2-17　“安全”选项卡

② 选中需要删除的权限，如 Users，单击“删除”按钮，删除 Users 访问权限。

③ 单击“确定”按钮，完成权限访问的设置。

这样系统磁盘 C 只有 SYSTEM 和 Administrators 的用户才具备访问的权限，可以有效地防止非授权用户的访问。

2.3.3　查看磁盘权限

微软公司提供了查看磁盘文件或者文件夹当前权限的图形化工具，名称为 AccessEnum，提供的下载地址为 http://download.sysinternals.com/Files/AccessEnum.zip，利用 AccessEnum 可全面了解文件系统和注册表安全设置，它是网络管理员查看安全权限的理想工具。

① 下载完成并解压缩后，直接执行 AccessEnum.exe 文件，即可启动程序。单击 Directory 按钮，显示“浏览文件夹”对话框。在对话框中选择需要查看的目标文件夹，此处以 C 盘为例，单击“确定”按钮，返回到运行窗口。继续单击 Scan 按钮，即可开始扫描，完成后显示如图 2-18 所示的

结果。

② 检测的结果以列表框的方式显示，分为 Path、Read、Write、Deny 这 4 个数据列。

■ Path：文件夹的路径。

■ Read：具备读权限的用户或者组。

■ Write：具备写权限的用户或者组。

■ Deny：具备拒绝权限的用户或者组。

③ 在扫描结果窗口中，双击对象名称即可打开其属性对话框，切换至如图 2-19 所示的“安全”选项卡即可查看详细权限设置，此处以 C:\目录为例。

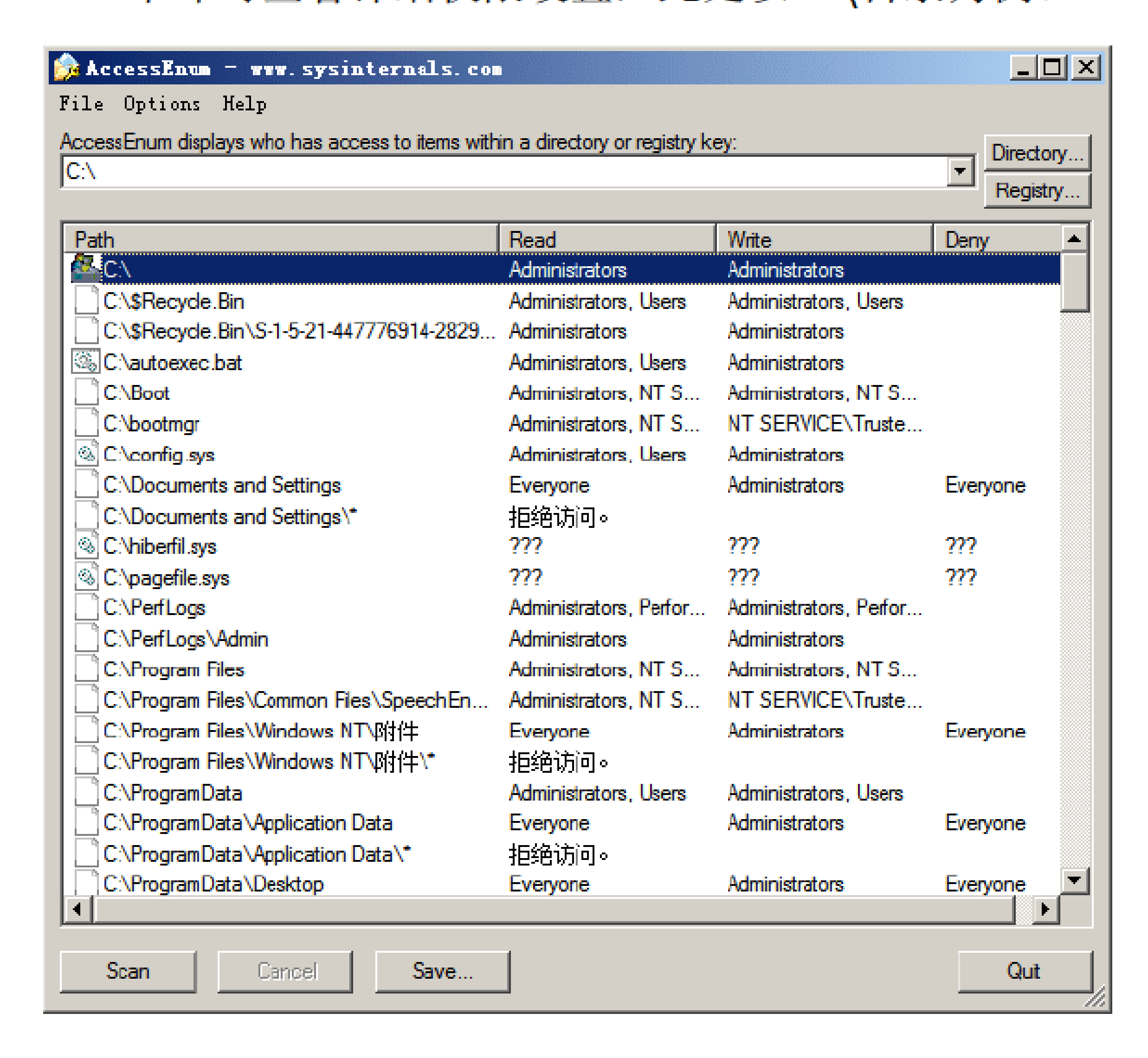


图 2-18 扫描结果

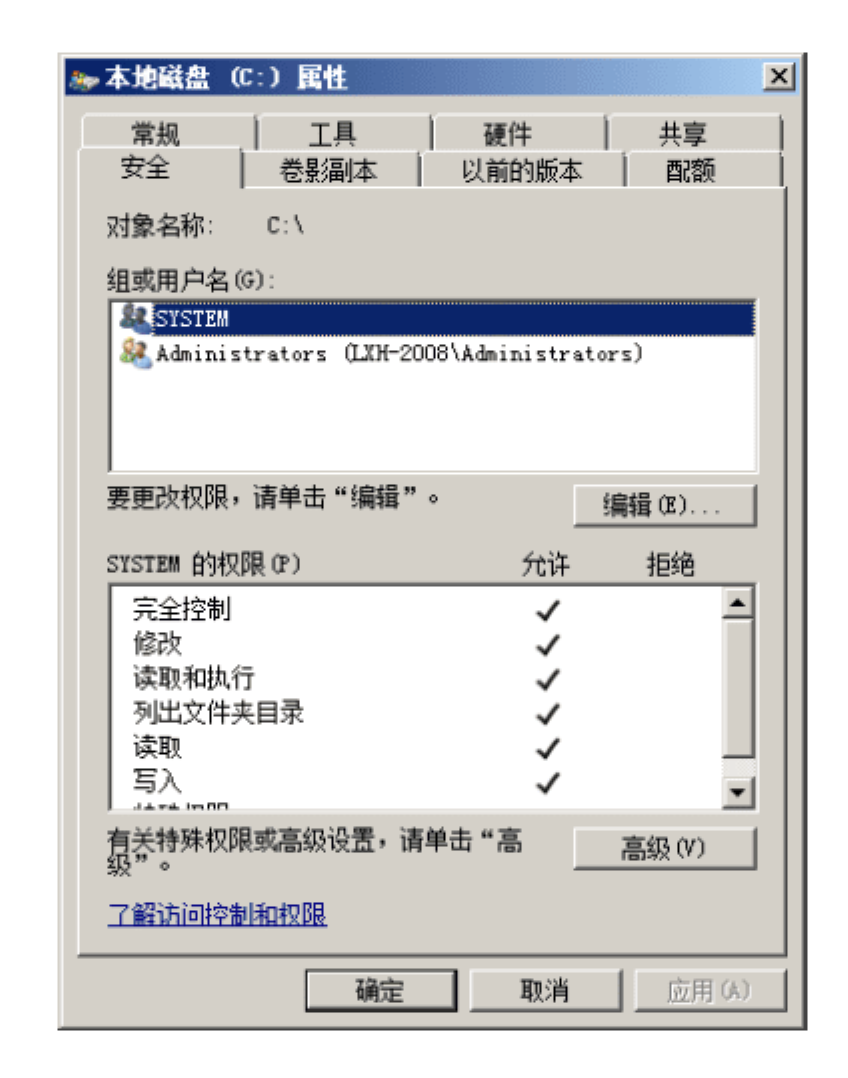


图 2-19 “安全”选项卡

④ 在“组或用户名”列表框中，添加或者删除需要赋予权限的用户或者组，单击“确定”按钮，完成权限的设置。

2.4 系统账户数据库

简单地讲，系统账户数据库就是 Windows Server 2008 系统中，用于存储用户账户信息的文件，包括账户名和密码等信息。默认情况下，系统已经自动对该文件进行加密，普通方法无法看到其真实内容，但使用一些工具软件就可以轻易查看。管理员可以借助系统提供的 Syskey 对文件进行二次加密，这样更能保证系统的安全，同时它还能设置启动密码，这个密码先于用户密码之前，因此起到双重保护的作用。

2.4.1 加密系统账户数据库

默认情况下，Windows Server 2003/2008 系统中所有用户账户的登录信息，全部保存在 %systemroot%\system32\config 目录下的 SAM 文件中，当然 Administrator 账户也不例外，这个 SAM 文件就是 Windows 的系统账号数据库。做好该文件的安全保护工作，也就间接保护了管理员账户的安全，通

常情况下可以通过加密方式实现。Syskey 是 Windows 系统内置的账户数据库加密专用工具，加密之后，即使入侵者窃取了被加密的 SAM 文件，也无法获取其中的用户名和密码信息。

① 单击“开始”按钮，在“开始”菜单的“开始搜索”文本框中输入“syskey”并按 Enter 键，打开如图 2-20 所示的“保证 Windows 账户数据库的安全”对话框。系统默认已经选择“启用加密”单选按钮，即始终执行对 SAM 文件的加密。直接单击“确定”按钮，将对 SAM 文件进行二次加密。

② 单击“更新”按钮，打开如图 2-21 所示的“启动密钥”对话框，系统默认选择“系统产生的密码”单选按钮。如果希望需要密码才能启动 Windows，则可以选择“密码启动”单选按钮，并设置一个安全性较高的密码，至少 12 个字符，最多可以为 128 个字符。

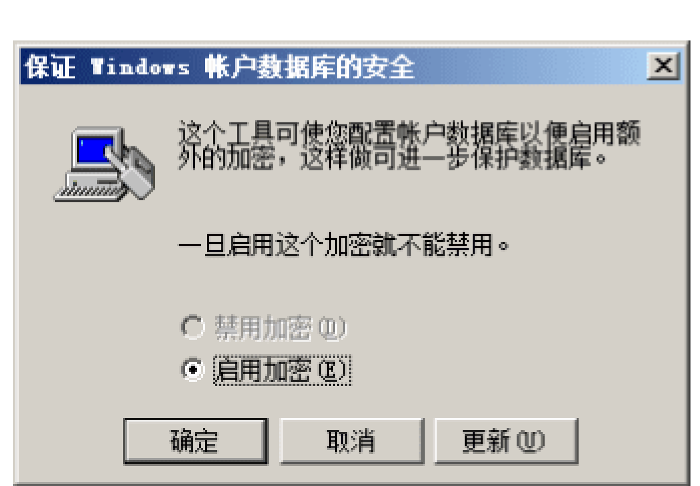




图 2-20　“保证 Windows 账户数据库的安全”对话框

图 2-21　“启动密钥”对话框

③ 单击“确定”按钮，显示如图 2-22 所示的“成功”对话框。

④ 单击“确定”按钮，保存设置。

通常情况下，系统产生的密码安全性要高于人工输入的密码，用户也可以依次选择“系统产生的密码”→“在软盘上保存启动密钥”单选按钮，打开如图 2-23 所示的“保存启动密钥”对话框。将已格式化好的空白软盘插入软驱并单击“确定”按钮，系统即可生成安全密码，并保存到软盘中。完成后提示如图 2-24 所示的对话框，启动系统时将提示插入该软盘。软盘中的密码文件默认名称为 StartKey.Key。



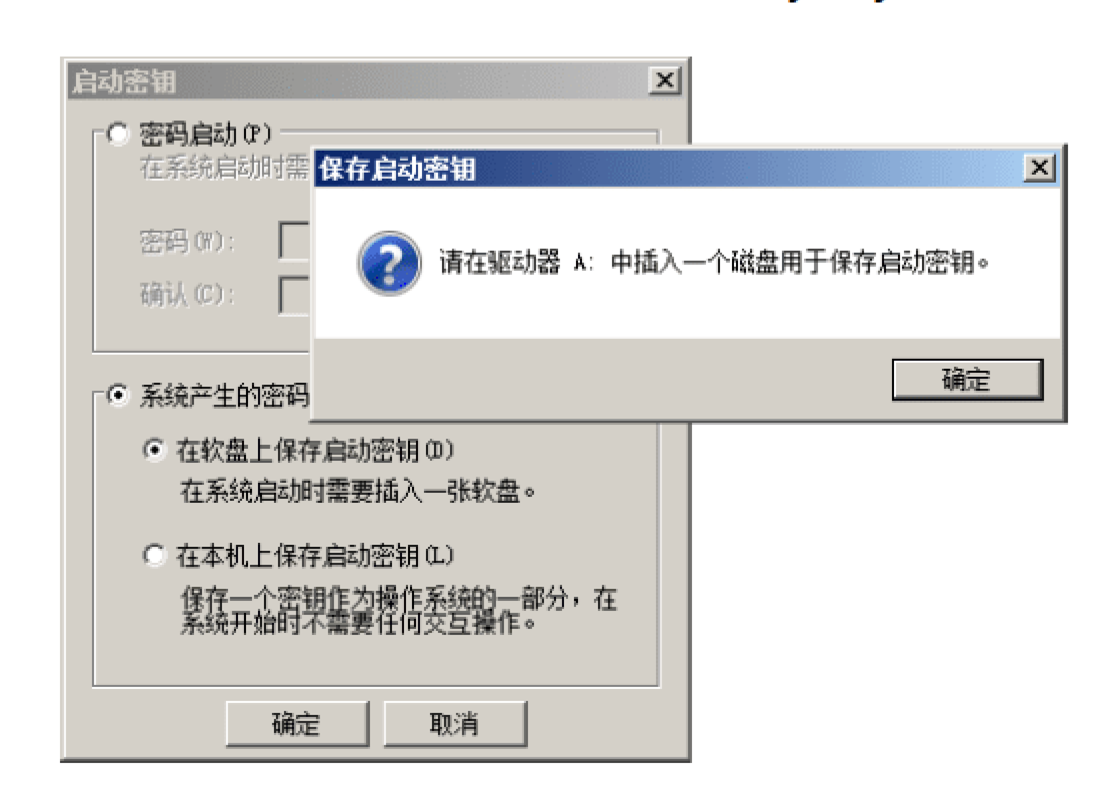


图 2-22　“成功”对话框

图 2-23　“保存启动密钥”对话框

如果将启动密码保存至软盘，则重新启动计算机时将显示如图 2-25 所示的“启动密钥盘”对话框，提示插入保存启动密码的软盘。

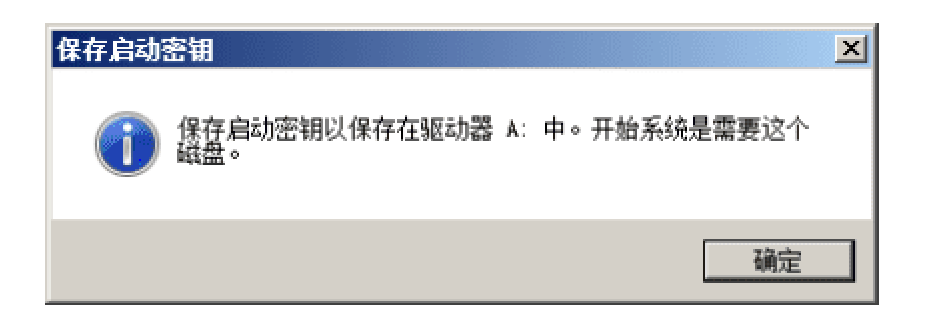




图 2-24　创建成功

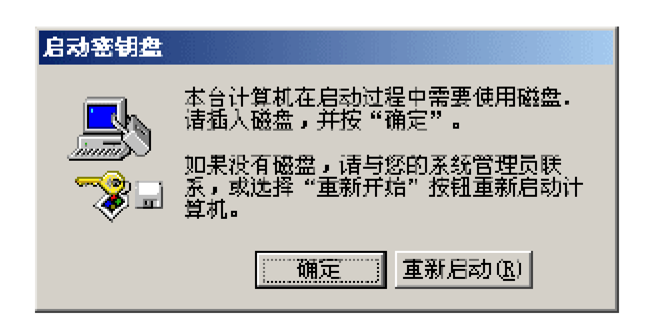


图 2-25　“启动密钥盘”对话框



注意：账户数据库的加密操作是不可逆的，即一旦启用将无法停止。但是如果不希望每次都要输入启动密码或准备启动密码软盘，可以直接在“启动密码”对话框中，依次选择“系统产生的密码”和“在本地机上保存启动密钥”单选按钮，将其恢复为默认状态即可。该选项是将保存一个密码作为操作系统的一部分，在系统开始时不需要用户进行任何交互操作，既安全又方便。

2.4.2　删除系统账户数据库

删除系统账户数据库是针对 SAM 文件的备份而言的，该操作仅适用于 Windows Server 2003，在 Windows Server 2008 中并不适用。按照默认方式安装 Windows Server 2003 后，将自动在%systemroot%\repair\目录下保存一份 SAM 备份，如图 2-26 所示。为防止原来密码的泄漏，需要删除该备份文件。

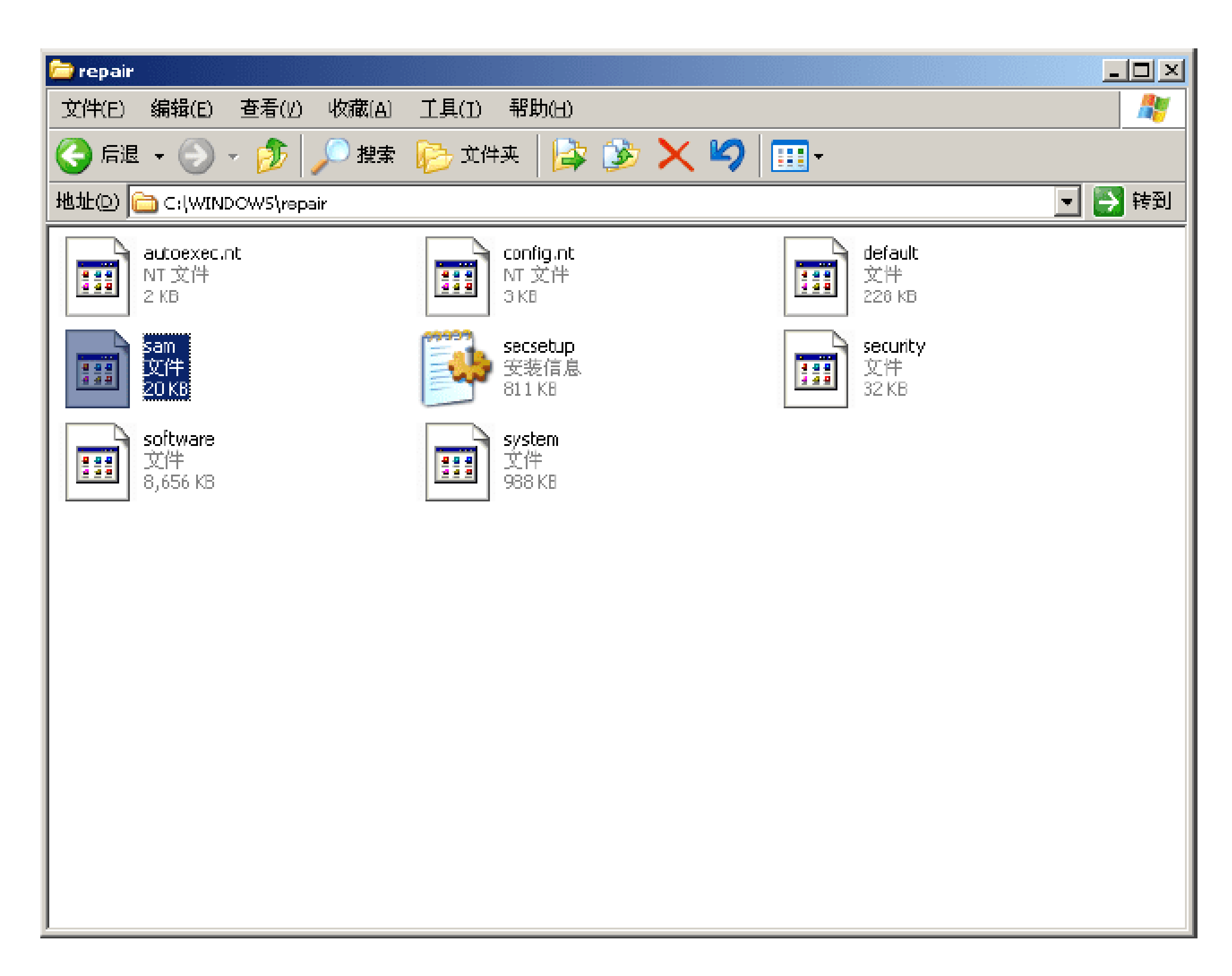


图 2-26　账号数据库的备份



提示：　使用 Syskey 加密后的密码无法使用逆反操作恢复账号的密码，备份文件将自动失效。

2.4.3　备份和恢复账户信息

credwiz 是 Windows Vista 和 Windows Server 2008 系统中新增的功能之一，可以帮助管理员备份和恢

复所有用户账户信息。通常情况下，Windows Server 2008 服务器上保存着所有客户端的用户账户信息，一旦遇到系统故障现象，这些信息很可能会被破坏或丢失。如果再使用手工方法重新录入每一个用户账户信息，不仅工作量大，而且容易出错。

① 单击“开始”按钮，在“开始搜索”文本框中，输入“credwiz”并按 Enter 键，显示如图 2-27 所示的“存储的用户名和密码”对话框，选择“备份存储的用户名和密码”单选按钮。

② 单击“下一步”按钮，显示如图 2-28 所示的“你想在什么位置备份存储的登录凭据”界面，单击“浏览”按钮，选择用于存储备份的目录，建议保存在软盘或移动磁盘上，并妥善保管，避免存储在本地计算机中。

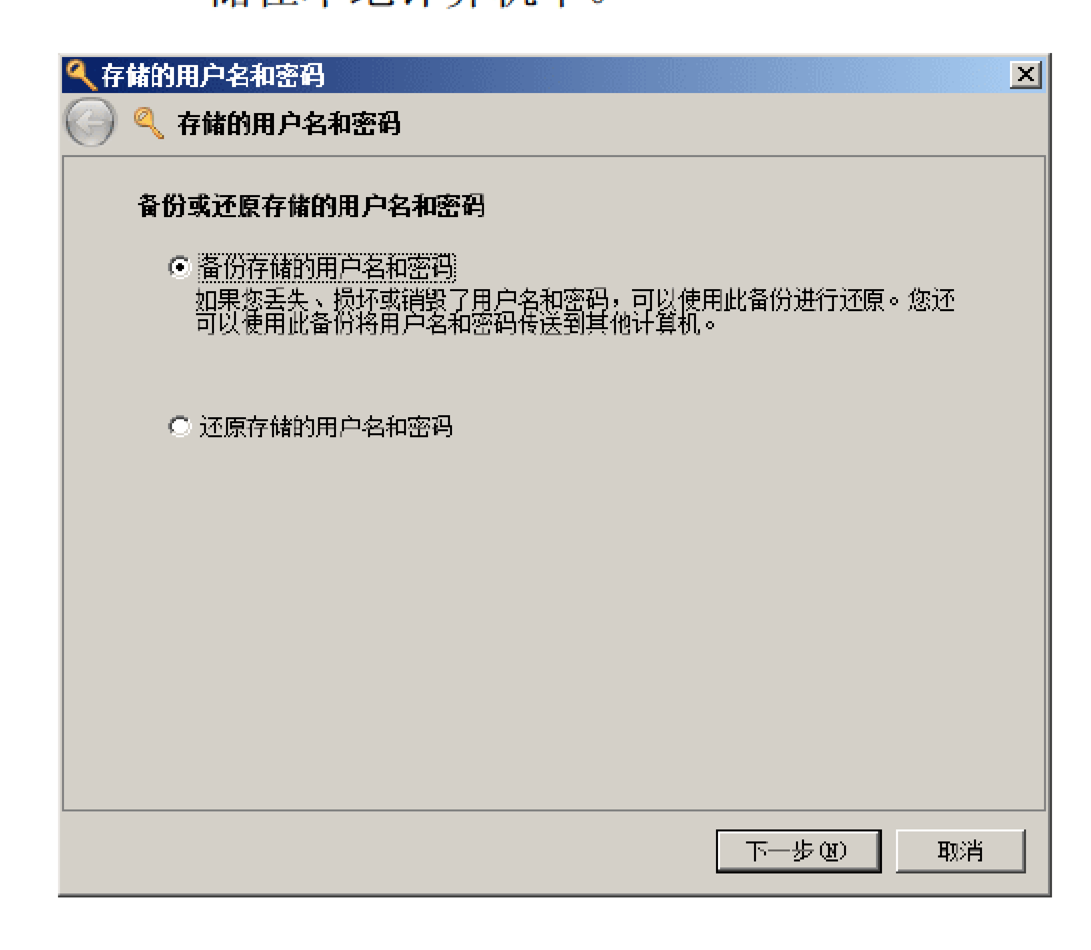


图 2-27　“存储的用户名和密码”对话框

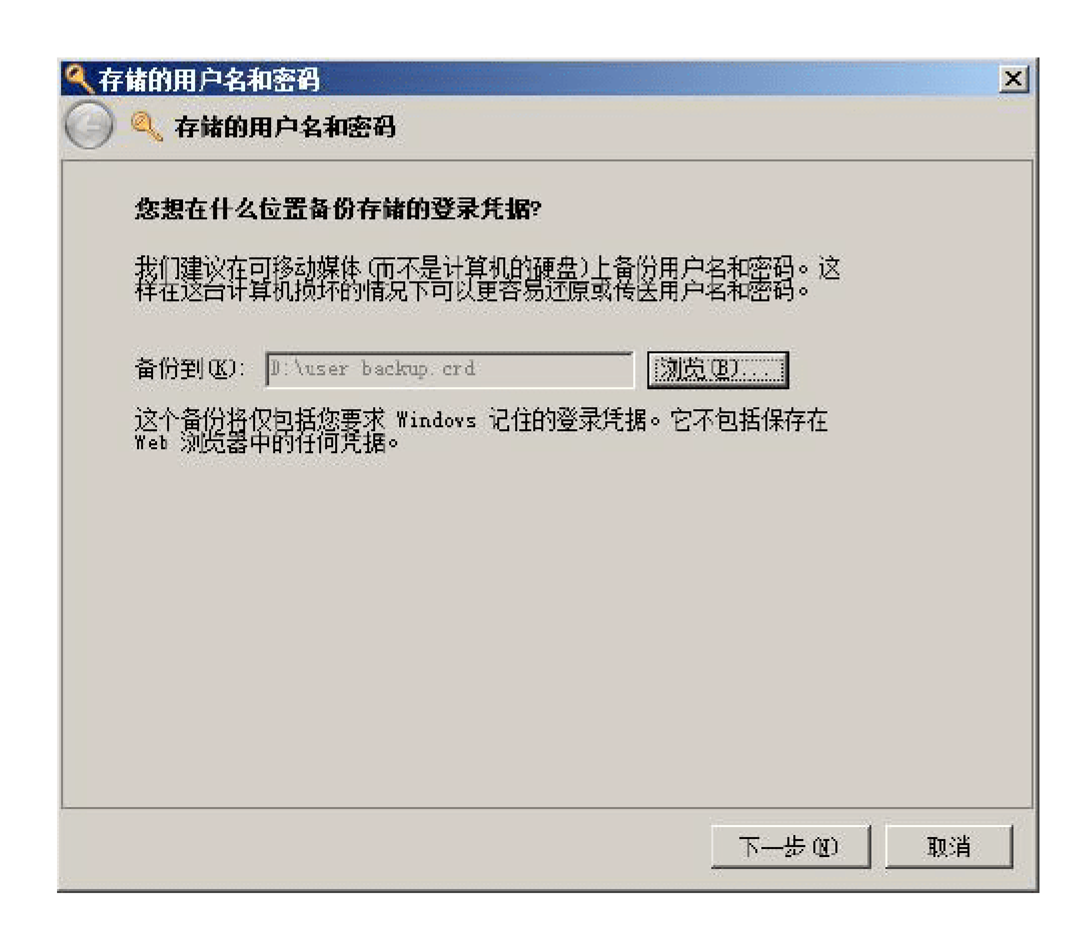


图 2-28　“你想在什么位置备份存储的登录凭据”界面

③ 单击“下一步”按钮，显示如图 2-29 所示的“按 CTRL+ALT+DELETE 继续在安全桌面上备份”界面。

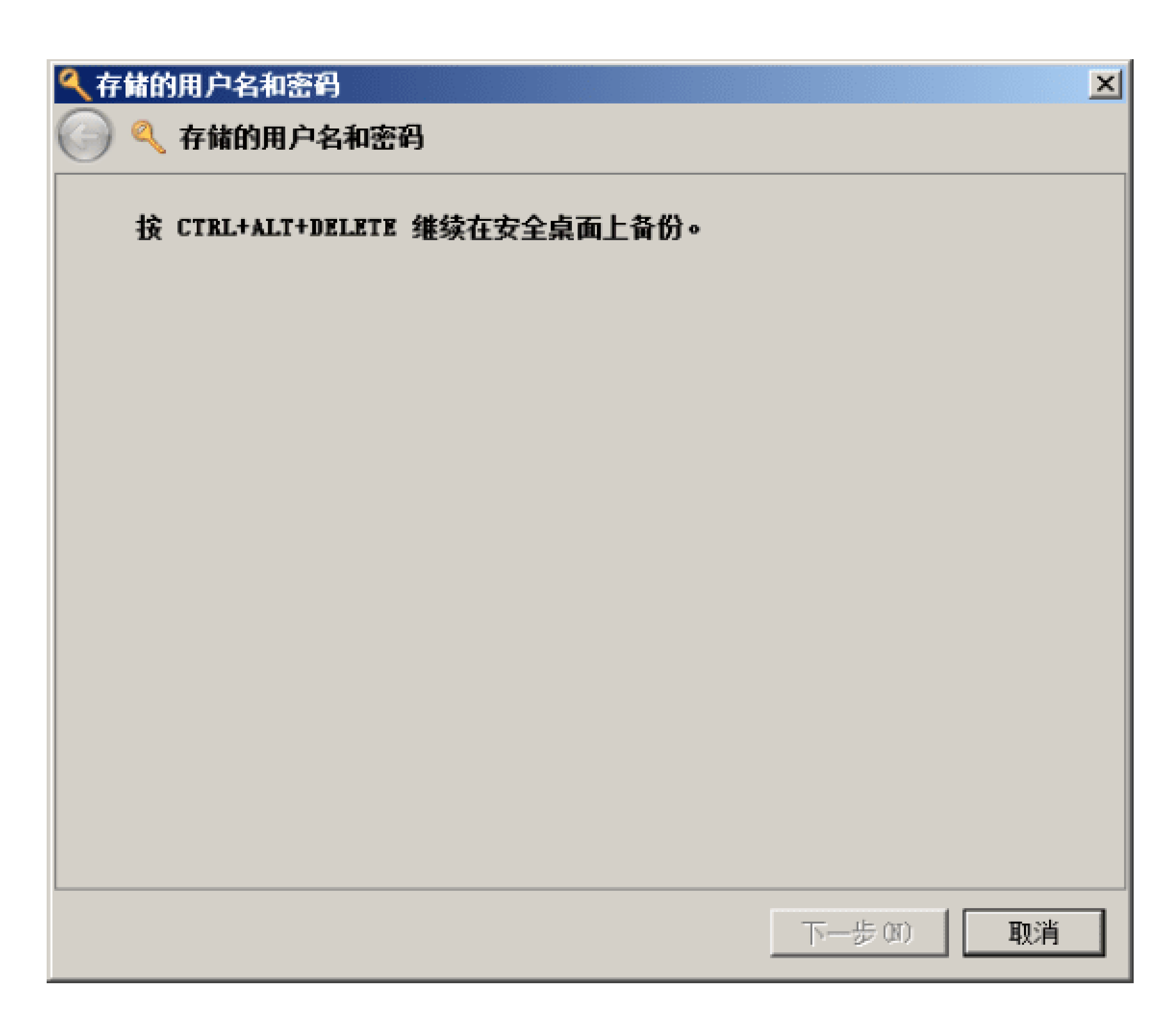


图 2-29　“按 CTRL+ALT+DELETE 继续在安全桌面上备份”界面

④ 根据提示信息，按 Ctrl+Alt+Delete 组合键，显示如图 2-30 所示的“使用密码保护备份文件”界

面，在“密码”和“确认密码”文本框中，输入欲使用的密码即可。该密码必须符合 Windows Server 2008 系统的安全密码复杂性要求。

⑤ 单击“下一步”按钮，显示如图 2-31 所示的“备份成功”界面。最后，单击“完成”按钮，关闭向导即可。



图 2-30 “使用密码保护备份文件”界面

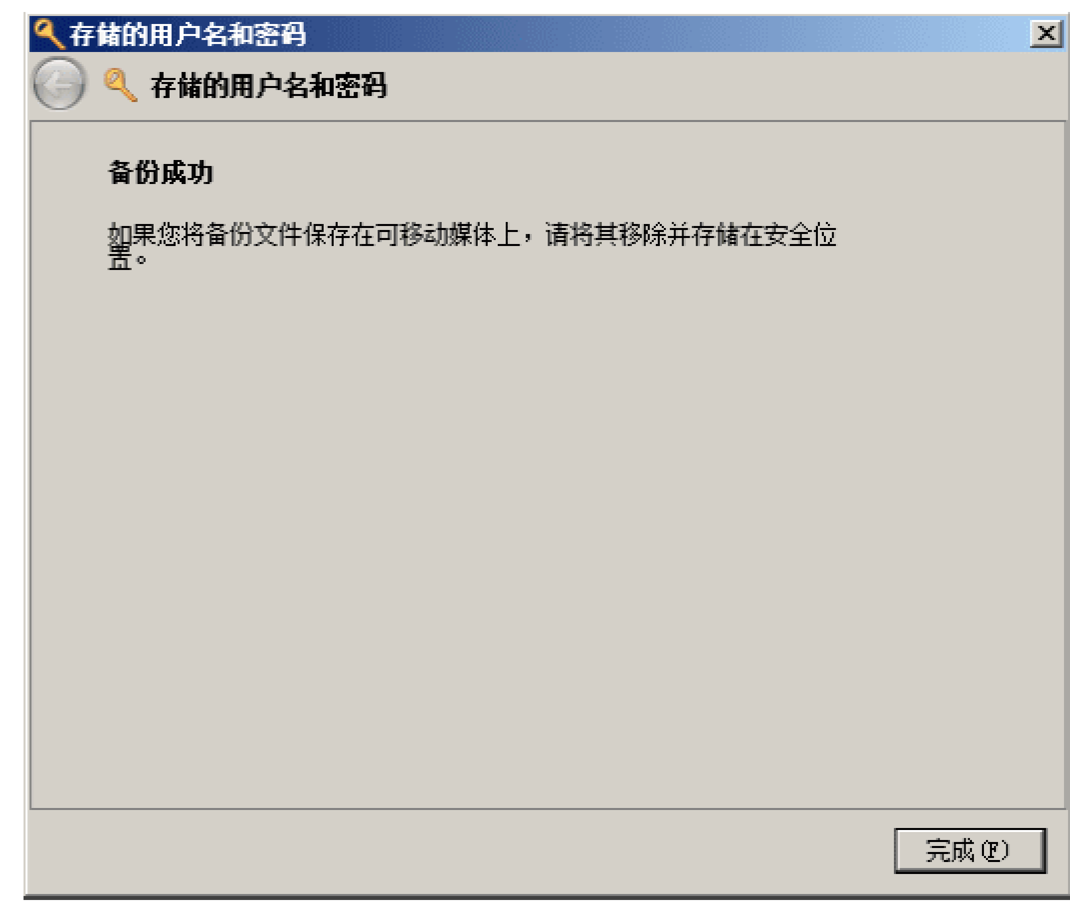


图 2-31 “备份成功”界面

完成备份操作后，存储在 Windows Server 2008 系统中的所有用户访问账号信息，都会被备份保存到指定位置处的 crd 文件中。当 Windows Server 2008 服务器系统出现故障导致用户信息丢失时，只需再次使用该命令的“还原存储的用户名和密码”功能，还原用户账户信息即可，需要注意的是，还原过程中需要提供备份时设置的加密密码。还原过程非常简单，这里不再详细介绍。

2.5 系统服务安全

系统服务对于服务器系统的重要性不言而喻，但是对于系统安全的意义也是非常重要的。所有系统应用都依赖于不同的服务，通过控制系统服务的状态，可以限制相应功能的开启或关闭，从而确保系统的安全。

2.5.1 常见服务攻击类型

由于 Windows 有很多默认服务在 Windows 启动时自动启动，入侵者经常以这些服务为跳板对系统进行攻击，例如冲击波、震荡波等。常见的 Windows 服务攻击方式包括如下几种。

1. 缓冲区溢出

缓冲区溢出是指当计算机向缓冲区内填充数据位数时，超过了缓冲区本身的容量，溢出的数据将覆盖原有合法数据。通常情况下，应用程序本身会自动检查数据长度，不允许输入超过缓冲区长度的字符，但是绝大多数程序都会假设数据长度与所分配的储存空间是完全匹配的，这就为缓冲区溢出埋下隐患。操作系统所使用的缓冲区又被称为堆栈，各个进程的指令会被临时储存在堆栈中，因此，堆栈也会出现缓冲区溢出。

2. 拒绝服务攻击

拒绝服务(DoS)攻击就是入侵者使目标主机停止提供服务或资源访问，包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。通常情况下，普通用户攻击很少单独使用 DoS 攻击破坏服务器，而只是将此类攻击作为入侵的一部分。例如，绕过入侵检测系统时，通常用大量的攻击触发检测系统，导致入侵检测系统日志过多或者反应迟钝，这样，入侵者就可以在潮水般的攻击中混过入侵检测系统。

3. 远程登录访问

许多基于 Windows 系统的服务都会提供额外登录点，例如 FTP、远程桌面、远程终端等，入侵者通常会通过反复尝试用户名和密码的方式，建立到服务器的连接，进而达到入侵的目的。如果没有对安全日志进行监视，入侵过程就很难被发现。

4. 窃听

在常规网络应用中，许多服务的用户账户信息都是以明文方式传输的，如 SNMP、Telnet、FTP 等，而一旦这些信息被入侵者截获，重要的用户账户登录信息就可能被窃取。不仅如此，一些使用密文传输的服务，也可能受到此类攻击，例如 RDP，即使通过加密，新会话也会被截获而传输给远程入侵者。窃听也可以用于捕获登录凭证之外的机密信息和个人信息。

5. 密码泄露

如果某入侵者拥有系统访问权限(如管理员或本地系统)，就会用各种方法和工具在明文中恢复登录账户凭据。如果将该凭据应用于其他的计算机，或应用于整个 Windows 域中，就会引起其他资源的泄露。

6. 配置错误

不合理的系统服务配置方式，也可能导致系统入侵事件的发生。例如，用户安装 IIS 或 FTP 服务，却使用简单的密码。

2.5.2　服务账户

服务仅在登录到某一账户的情况下才能访问操作系统中的资源和对象。大多数的服务都不更改默认的登录账户，更改默认账户可能导致服务失败。如果选定账户没有登录计算机服务的权限，Microsoft 管理控制台(MMC)的服务管理单元将自动为该账户授予登录服务的用户权限，但并不一定会启动服务。

1. 本地系统账户

本地系统账户功能强大，它可对本地系统进行完全访问，并为网络中的计算机提供服务。如果某服务登录到域控制器使用的“本地系统”账户，则该服务可访问整个域。有些服务的默认配置使用的是“本地系统”账户，则不需要更改默认服务设置。本地系统账户名称是 LocalSystem，没有密码设置。

2. 本地服务账户

本地服务账户是一种特殊的内置账户，类似于经过身份验证的用户账户。就访问资源的对象而言，“本地服务”账户与“Users”(用户)组成员权限等同。这种限制性访问有助于在个别服务或进程受损时保障系统安全，以“本地服务”账户运行的服务使用有匿名凭据的空会话来访问网络资源。账户名称为 NTAUTHORITY\LocalService，该账户没有密码。

3. 网络服务账户

网络服务账户也是一种特殊的内置账户，类似于经身份验证的用户账户。就访问资源的对象而言，“网络服务”账户与“Users”(用户)组成员权限等同。这种限制性访问有助于在个别服务或进程受损时保障系统安全，以“网络服务”账户运行的服务可以使用计算机账户的凭据来访问网络资源。账户名称为NTAUTHORITY\NetworkService，该账户没有密码。



注意： 如果更改默认服务设置，重要的服务可能无法正常运行。最重要的是，更改启动类型一定要谨慎，要使用配置了自动启动服务的设置来登录。

2.5.3 服务权限

每个服务都有特定的权限，管理员可以将这些权限授予每一个用户或组，也可以从用户或组的权限中取消相应的服务权限。服务具有的权限及描述如表 2-1 所示。

表 2-1 服务权限及描述

权　限	描　述
完全控制	执行所有功能。默认情况下，服务会自动授予登录用户完全控制权限
查询模板	确定与某个服务对象关联的配置参数
更改模板	更改服务的配置，如更改启动类型
状态查询	有关服务状态的访问信息
列举依存关系	确定依存于指定服务的所有其他服务
启动	启动服务
停止	停止服务
暂停和继续	暂停或继续服务
询问	报告服务的当前状态信息
用户定义的控制	将用户定义的控制请求或特定于服务的请求发送给该服务
删除	删除服务
读取权限	读取指派给服务的安全权限
更改权限	更改指派给服务的安全权限
取得所有权	更改安全密钥，或更改关于不为用户所有的服务的权限

2.5.4 漏洞和应对措施

任何服务或应用程序都是潜在的攻击点，因此，必须禁用或删除系统环境中不需要的服务或可执行文件，或者直接删除闲置的网络服务。通常情况下，为服务设置适当的启动方式，是避免服务漏洞攻击的首选方式。Windows Server 2008 系统服务提供如下 4 种启动方式。

- 自动。此服务随着系统启动时启动，延长启动所需要的时间，有些服务是必须设置为自动的，如 Remote Procedure Call(RPC)。由于依存关系或其他影响，其他的一些服务也必须设置为自动，这样的服务最好不要去更改它，否则系统无法正常运行。

- 手动。如果某系统服务被设置为手动启动方式，则用户可以在需要时再运行它。以便节省大量的系统资源，加快系统启动。
- 已禁用。此类服务不能再运行。这个设置一般在提高系统安全性时使用。如果怀疑一个陌生的服务会给当前系统带来安全隐患，则可以先尝试停止它，看看系统是否能正常运行。如果一切正常，则就可以直接禁用。如果以后需要这个服务，在启动它之前，必须先将启动类型设置为自动或手动。
- 自动(延迟的启动)。这是 Windows Vista 和 Windows Server 2008 系统中新增的控制方式，其作用是延缓服务的启动，以减小系统载入时的负荷，使系统尽快进入用户响应状态后再启动某些关键的服务。由于许多系统服务之间都存在依存关系，建议慎重选择该选项，以免设置不当导致系统启动故障。

对于所有非必要的服务应当禁用。除此之外，还可通过配置用户定义账户列表的访问控制列表(ACL)来编辑服务安全性。

虽然禁用不必要的服务可以减少系统资源的占用以及系统漏洞，但有些服务(例如 Security Accounts Manager)禁用后将导致系统无法引导，禁用一些关键服务可能使计算机无法通过域控制器的身份验证。因此，为安全起见，在禁用系统服务前应先在测试环境中测试。

2.5.5 配置系统服务安全

默认情况下，大多数系统服务的登录账户都是“本地系统账户”。如有特殊需要，可按照如下步骤更改为其他账户。

① 依次单击“开始”→“管理工具”→“服务”，打开“服务”窗口。双击需要更改登录账户的服务(如 Windows Installer 服务)，打开服务属性对话框，切换至如图 2-32 所示的“登录”选项卡，默认选择“本地系统账户”单选按钮。

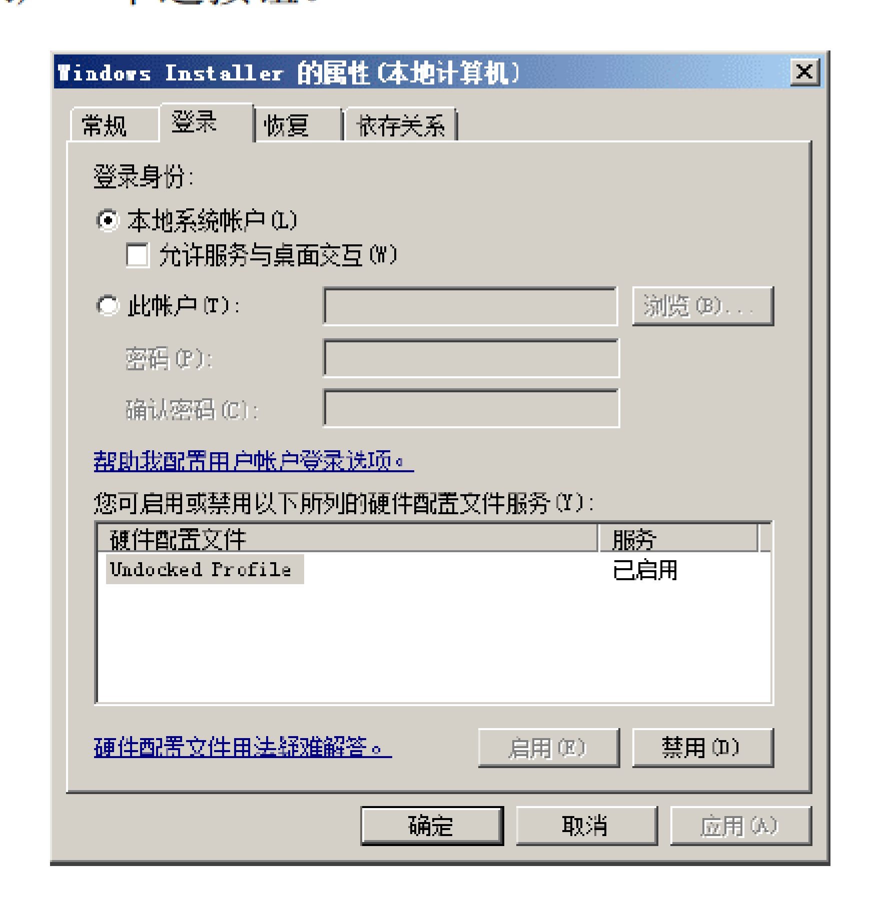


图 2-32 “登录”选项卡

注意：建议不要选中“允许服务与桌面交互”复选框。如果允许服务与桌面交互，则服务在桌面上显示的任何信息也都会显示在交互用户的桌面上。恶意用户可能会获得对该服务的控制权，或从交互桌面攻击它。

② 选择“此账户”单选按钮，单击“浏览”按钮，打开“选择用户”对话框，在“输入要选择的对象名称”文本框中输入想要设置的登录账户，如图 2-33 所示。也可以单击“高级”按钮，从用户列表中搜索目标账户。

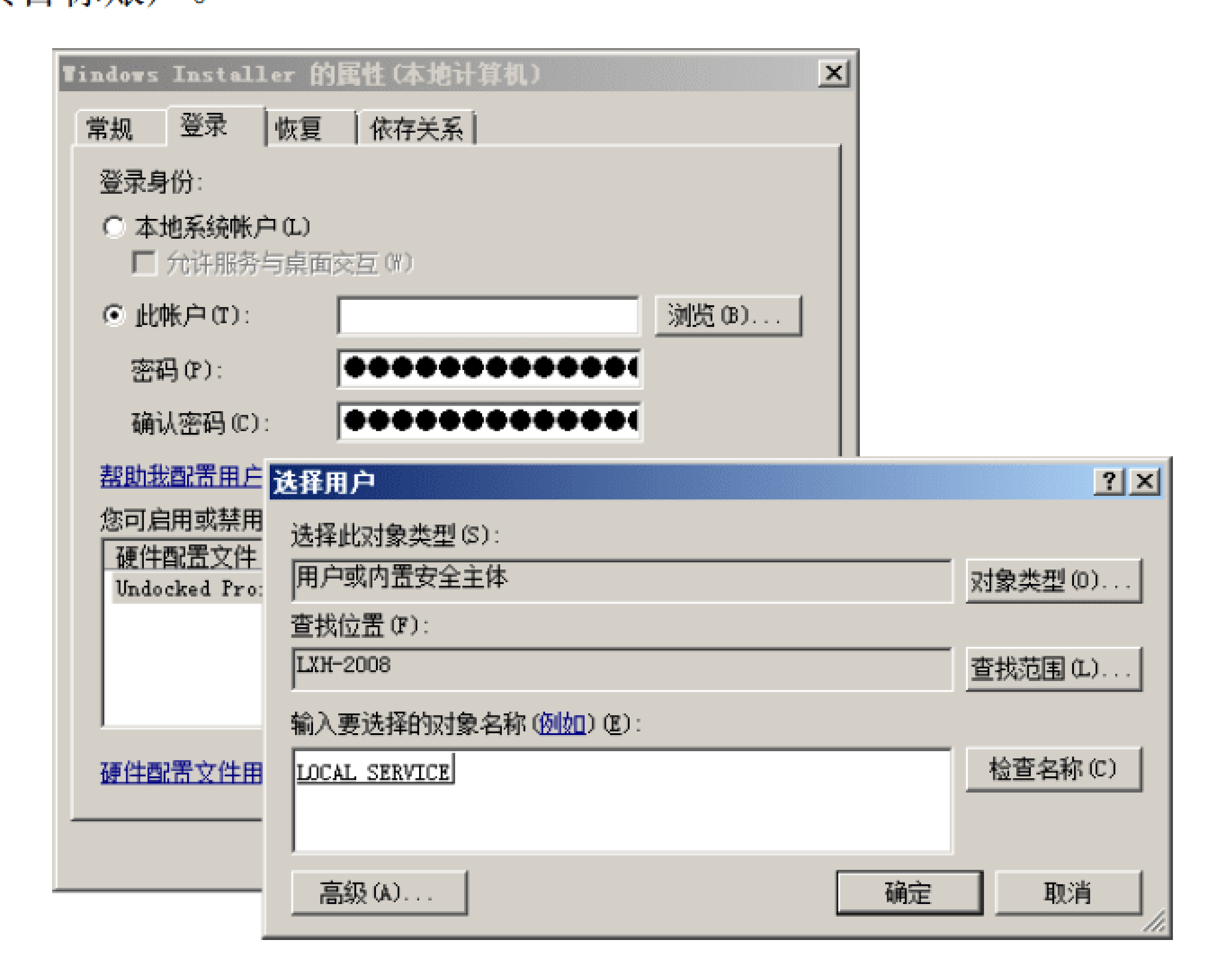


图 2-33　更改账户

③ 单击“确定”按钮，即可将所选账户添加到“此账户”文本框中。本例中使用的 Local Service 账户，密码必须为空，如图 2-34 所示。如果选择其他账户。则在“密码”和“确认密码”文本框中输入用户账户的密码即可。

④ 单击“应用”按钮，显示如图 2-35 所示对话框，提示已经成功授予用户账户“以服务方式登录”的权利。




图 2-34　“此账户”已添加



图 2-35　登录账户更改成功

⑤ 单击“确定”按钮，保存设置即可。需要注意的是，必须重启服务才可使更改生效。

2.5.6 系统服务详解

管理员虽然不必详细了解每一项系统服务的安全配置，但为了确保必要系统服务正常运行，往往还需要一些附加服务，因此，管理员应简要了解重要系统服务的主要功能，以及与其他系统服务间的依附关系。默认情况下，Windows Server 2008 系统提供如表 2-2 所示的系统服务。

表 2-2 Windows Server 2008 系统服务详解

服务名称	功 能	默认状态	推荐设置
Application Experience	该服务主要用于为系统与一些旧版本或存在兼容性问题的应用程序提供解决方案，如果服务器上没有运行此类程序，则不必启动该服务	自动	手动
Application Information	启用该服务即可使用 Administrator 权限安装旧版本的软件，配合 UAC(User Account Control，用户账户控制)使用，可以防止木马和不知名的病毒安装程序入侵	手动	手动
Application Layer Gateway Service	为特殊应用软件提供服务，例如 Windows 防火墙，主要是为 Internet 连接提供第三方协议插件支持。在大多数情况下，该服务会随着其他服务自动启动	手动	手动
Application Management	主要用于提供集中式管理，例如使用活动目录分发软件等，如果是独立服务器，建议关闭该服务	手动	手动
Background Intelligent Transfer Service	用于 Windows 系统自动更新，以便在后台传输补丁程序，如果不使用 Windows Update 可以关闭	自动(延迟的启动)	自动
Base Filtering Engine	主要是为系统安全方面提供服务，如防火墙、远程连接、Internet 连接共享以及一些不常用的协议都需要使用该服务，建议设置为“自动”方式	自动	自动
Block Level Backup Engine Service	用于 Windows Server 2008 备份及恢复，可以根据需要开启或关闭	手动	手动
Certificate Propagation	使用 VPN 接入方式的网络要求使用 Smart Cards，该服务是 Smart Cards 服务所必需的，如果没有这方面的需求，特别是个人用户可以关闭	手动	禁用
CNG Key Isolation	如果启动 Wired AutoConfig 和 WLAN AutoConfig 两个服务，而且使用了 EAP (Extensible Authentication Protocol，扩展认证协议)，则该服务将自动启动。如果不使用自动网络配置方式，则可以关闭该服务	手动	手动
COM+ Event System	支持系统事件通知服务(SENS)，此服务为订阅的组件对象模型(COM)组件提供自动分布事件功能。如果停止此服务，SENS 将关闭，而且不能提供登录和注销通知。如果禁用此服务，依赖此服务的其他服务都将无法启动	自动	自动
COM+ System Application	管理 COM+组件的配置和跟踪。如果停止该服务，则大多数基于 COM+的组件将不能正常工作。该服务通常用于应用程序开发，如 COM+程序、.NET 程序等	手动	手动

续表

服务名称	功　能	默认状态	推荐设置
Computer Browser	提供浏览局域网计算机的功能，如果关闭该服务，将无法访问局域网，并且任何直接依赖于此服务的服务将无法启动	禁用	手动
Cryptographic Services	维护和管理系统的所有证书、密钥以及安全数据库。另外访问一些网站所需要的服务，例如访问微软网站、Windows Update 或者 DRM 网站等，都需要使用该服务。如果关闭该服务，则这些管理服务将无法正常运行，任何依赖它的服务也将无法启动	自动	自动
DCOM Server Process Launcher	为 DCOM 服务提供加载功能，是 Windows Server 2008 系统的基本服务，建议慎重配置	自动	自动
Desktop Window Manager Session Manager	提供桌面窗口管理器启动和维护服务，所有 Aero Glass 和 Flip 3D 效果均依赖该服务	自动	手动
DHCP Client	为此计算机注册并更新 IP 地址，如果启用“自动获取 IP 地址”配置方式，则必须启动该服务，否则计算机将不能接收动态 IP 地址和 DNS 更新	自动	自动(启动的延迟)
Diagnostic Policy Service	提供 IE 7.0 的故障诊断、排除和解决方案。如果该服务被停止，诊断将不会继续正常运行，其他依赖于该服务的服务也将无法启动	自动	禁用
Diagnostic Service Host	配合 Diagnostic Policy Service 服务完成一些具体工作，如果停止该服务，一些系统诊断功能也将无法顺利完成	手动	禁用
Diagnostic System Host	为 Windows 系统组件提供故障诊断和解决方案	手动	禁用
Distributed Link Tracking Client	维护某个计算机内或某个网络中的计算机的 NTFS 文件之间的链接，如果服务器使用的是 NTFS 文件系统，则必须启动该服务	自动	禁用
Distributed Transaction Coordinator	协调跨多个数据库、消息队列、文件系统等资源管理器的事务。如果停止此服务，则不会发生这些事务	自动(延迟的启动)	手动
DNS Client	DNS 客户端服务用于缓存域名系统名称并注册该计算机主机名称。如果该服务被停止，将继续解析 DNS 名称，即无法访问 Internet	自动	自动
Extensible Authentication Protocol	可扩展验证协议主要提供 802.1x 有线和无线、VPN 和网络访问保护功能。EAP 在身份验证过程中也提供网络访问客户端使用的应用程序编程接口(API)，包括无线客户端和 VPN 客户端。如果禁用此服务，该计算机将无法访问需要 EAP 身份验证的网络	手动	手动
Function Discovery Provider Host	功能发现提供程序的主机进程，与 PnP-X 和 SSDP 服务相互关联	手动	手动
Function Discovery Resource Publication	发布该计算机以及连接到该计算机的资源，以便能够在网络上发现这些资源。如果该服务被停止，将不再发布网络资源，网络上的其他计算机将无法发现这些资源	自动	手动
Group Policy Client	为系统提供组策略管理功能，如果停止或禁用该服务，将无法应用设置，并且将无法通过组策略管理应用程序和组件	自动	手动

续表

服务名称	功　能	默认状态	推荐设置
Health Key and Certificate Management	为网络访问保护代理提供 X.509 证书和密钥管理服务。如果关闭该服务，则无法使用 X.509 证书功能	手动	手动
Human Interface Device Access	启用对智能界面设备(HID)的通用输入访问，激活并保存键盘、远程控制和其他多媒体设备上的预先定义的热键。如果此服务被终止，由此服务控制的热键将失效	手动	手动
IKE and AuthIP IPSec Keying Modules	该服务托管 Internet 密钥交换和身份验证 Internet 协议键控模块。这些键控模块用于 Internet 协议安全中的身份验证和密钥交换。停止或禁用该服务将禁用与对等计算机的 IKE/AuthIP 密钥交换，建议运行 IKEEXT 服务	自动	自动
Interactive Services Detection	启用交互式服务的用户输入的用户通知，这样当交互式服务创建的对话框出现时可以访问这些对话框。如果此服务已停止，将不再有新的交互式服务对话框通知，而且可能再也无法访问交互式服务对话框	手动	手动
Internet Connection Sharing (ICS)	为办公网络提供网络地址转换、寻址、名称解析和入侵保护服务，主要功能是网络连接共享。如果不是这种方式接入 Internet，则可以关闭	禁用	禁用
IP Helper	在 IPv4 网络上提供自动的 IPv6 连接。如果停止此服务，则在计算机连接到本地 IPv6 网络时，该计算机将只具有 IPv6 连接。如果只连接 IPv4 网络，则无需启用该服务	自动	手动
IPSec Policy Agent	Internet 协议安全支持网络级别的对等身份验证、数据原始身份验证、数据完整性、数据机密性以及重播保护。如果所在网络中无需配置安全策略，则可以关闭该服务。此服务停止时，Windows 防火墙的远程管理也不再可用	自动	手动
KtmRm for Distributed Transaction Coordinator	协调分布式传输协调程序(MSDTC)和核心事务管理器(KTM)之间的事务，主要用于为系统开发人员提供服务。普通用户可以设置为“手动”状态	自动(延迟启动)	手动
Link-Layer Topology Discovery Mapper	支持 LLTD 技术，可以精确地显示支持 LLTD 的设备在网络结构中的位置。创建网络映射，它由 PC 和设备拓扑信息以及说明每个 PC 和设备的元数据组成	手动	手动
Microsoft .NET Framework NGEN v2.0.50727_X86	为 NGEN 的应用提供支持，目前主要用于.NET 程序开发，将来还可以为基于.NET FX3 的程序开发提供支持，保持默认设置即可	手动	手动
Microsoft Fibre Channel Platform Registration Service	注册带有所有可用光纤通道纤维的平台，并维护这些注册	手动	手动
Microsoft iSCSI Initiator Service	管理本计算机以及到远程 iSCSI 目标设备的 Internet SCSI 会话。如果当前服务器没有 iSCSI 设备，也不需要连接和访问远程 iSCSI 设备，则可以关闭该服务	手动	手动

续表

服务名称	功　能	默认状态	推荐设置
Microsoft Software Shadow Copy Provider	管理卷影复制服务制作的基于软件的卷影副本。如果关闭该服务，将无法管理基于软件的卷影副本	手动	手动
Multimedia Class Scheduler	主要为本地计算机的多媒体应用提供服务，如视频、音频文件播放。关闭该服务可能会导致声卡出现故障	自动	自动
Netlogon	为用户和服务身份验证维护此计算机和域控制器之间的安全通道。如果关闭该服务，则计算机可能无法验证用户和服务身份并且域控制器无法注册 DNS 记录	手动	手动
Network Access Protection Agent	在客户端计算机上启用网络访问保护功能，即配置 NAP 客户端	手动	手动
Network Connections	管理“网络和拨号连接”文件夹中对象，管理员可以查看局域网和远程连接，或者访问网络资源	手动	自动
Network List Service	识别计算机已连接的网络，收集和存储这些网络的属性，并在更改这些属性时通知应用程序	自动	自动
Network Location Awareness	收集和存储网络的配置信息，并在此信息被修改时向程序发出通知。如果关闭此服务，则配置信息将不可用	自动	手动
Network Store Interface Service	该服务支持 NLA 服务，向用户模式客户端发送网络通知(例如，添加/删除接口等)。关闭该服务将导致丢失网络连接	自动	手动
Offline Files	脱机文件服务可以为本地计算机上打开的远程共享资源提供缓存，该服务是实现公共 API 的内部部分，并将相关的事件分配给关心脱机文件活动和缓存更改的用户	禁用	手动
Performance Logs & Alerts	为系统性能日志和警报功能提供支持，对于服务器而言收集远程计算机的性能数据也需要用到该服务。需要注意的是该服务可能会占用较多的系统资源，应根据需要开启或关闭	手动	手动
Plug and Play	该服务用于提供即插即用功能，使计算机在极少或没有用户介入的情况下可以识别并适应硬件的更改。关闭该服务会造成系统不稳定	自动	自动
PnP-X IP Bus Enumerator	PnP-X 总线枚举器服务管理虚拟网络总线，该服务是即插即用的扩展，使用 SSDP/WS 发现协议来发现网络连接设备并使其存在于 PnP 中，如能联网的电饭锅、冰箱等。如果停止或禁用此服务，则 NCD 设备将不会继续保持在 PnP 中。所有基于 PnP-X 的方案都将停止运行	禁用	禁用
Portable Device Enumerator Service	该服务的主要功能是，使 Windows Media Player 和移动媒体播放器(如 MP3)进行数据和时钟同步	手动	手动
Print Spooler	该服务允许将文件加载到内存供稍后打印，如果不需本地或任何网络打印机，则可以关闭该服务	自动	手动
Problem Reports and Solutions Control Panel Support	此服务为查看、发送和删除“问题报告和解决方案”控制面板的系统级问题报告提供支持，一般情况下作用不大	手动	手动

续表

服务名称	功 能	默认状态	推荐设置
Protected Storage	为敏感数据(如密码)提供保护存储，以防止未授权的服务、进程或用户访问	手动	手动
Remote Access Auto Connection Manager	当本地计算机引用一个远程 DNS 或 NetBIOS 名或者地址时，就会创建一个到远程网络的连接，例如 VPN 远程访问等。如果关闭该服务，将无法建立远程网络连接	手动	手动
Remote Access Connection Manager	管理从这台计算机到 Internet 或其他远程网络的拨号和 VPN 连接。如果禁用该项服务，则明确依赖该服务的任何服务都将无法启动	手动	手动
Remote Procedure Call (RPC)	为 COM 和 COM+的运行提供支持。如果关闭该服务，使用 COM 或远程过程调用(RPC)服务的程序将无法正常工作	自动	自动
Remote Procedure Call (RPC) Locator	配合 RPC 的服务，并管理本地 RPC 名称服务数据库	手动	手动
Remote Registry	使远程用户能修改此计算机上的注册表设置。如果关闭该服务，则只能在本地计算机上修改注册表	自动	手动
Resultant Set of Policy Provider	提供网络服务，即处理在不同情况下模拟应用目标用户或计算机的组策略设置的请求，并计算组策略设置的结果集	手动	手动
Routing and Remote Access	提供路由和远程访问功能，在局域网以及广域网环境中为企业提供路由服务	禁用	禁用
Secondary Logon	该服务允许多个用户同时登录到当前服务器，对于需要接受远程管理的服务器而言非常实用	自动	手动
Secure Socket Tunneling Protocol Service	该服务提供使用 VPN 连接到远程计算机的 SSTP 方式的支持。如果该服务被禁用，则用户将无法使用 SSTP 访问远程服务器	手动	手动
Security Accounts Manager	提供系统的安全账户管理服务，关闭该服务后将无法应用系统提供的安全账户管理器(SAM)加密本地账户	自动	自动
Server	确保本地计算机发布到网络上的共享资源，可以被顺利访问，如共享文件、打印机等。如果关闭该服务，网络用户将无法访问该服务器上的共享资源	自动	手动
Shell Hardware Detection	为自动播放硬件事件提供通知，如多媒体光盘或其他移动存储介质等	自动	手动
SL UI Notification Service	提供软件授权激活和通知，和 Software Licensing 一起是用于 Windows Server 2008 或其他一些软件激活服务	手动	手动
Smart Card	管理此计算机对智能卡的读取访问，如果企业网络启用的用户验证方式为智能卡，则应启用该功能。如果此服务被终止，此计算机将无法读取智能卡	手动	手动
Smart Card Removal Policy	允许系统配置为移除智能卡时锁定用户桌面。例如，如果希望在用户拿走智能卡之后计算机锁定，那么打开这个服务	手动	手动

续表

服务名称	功　能	默认状态	推荐设置
SNMP Trap	收集本地或远程计算机的 SNMP 信息，并将其转发给本机的 SNMP 管理程序。如果关闭该服务，此计算机上基于 SNMP 的程序将不会接收 SNMP 陷阱消息	手动	手动
Software Licensing	负责 Vista 系统的 License 管理和验证以及提供接口和 API 服务，供 Windows 系统或其他应用程序使用。Vista 的新增特性均会使用这个服务，如果禁用该服务，操作系统和许可的应用程序可能以缩减功能模式运行	自动	自动
Special Administration Console Helper	允许管理员使用紧急管理服务远程访问命令行提示符	手动	手动
SSDP Discovery	该服务在网络中搜索使用了 SSDP 发现协议的一些设备，比如一些非即插即用的设备，也会在设备管理中枚举本机上的非即插即用设备。如果停止此服务，基于 SSDP 的设备将不会被发现	禁用	禁用
Superfetch	维护和提高一段时间内的系统性能，非常实用	禁用	禁用
System Event Notification Service	SENS 提供了一个唯一的系统追踪、通知的机制，使其用于系统的登录、设备连接、网络连接、电源和内部事件的订阅及通知	自动	手动
Task Scheduler	该服务提供定制任务功能，Windows 系统或第三方应用程序都需要用到该服务。如果关闭该服务，则用户将无法完成任何定制任务	自动	自动
TCP/IP NetBIOS Helper	主要是支持 NetBIOS 名称的解析，从而使用户能够共享文件、打印和登录到网络。如果关闭服务，这些功能可能不可用	自动	手动
Telephony	提供电话服务 API 支持，以便各程序控制本地计算机上的电话服务设备以及通过 LAN 同样运行该服务的服务器上的设备	自动	自动
Terminal Services	允许用户以交互方式连接到远程计算机，如远程桌面、远程协助、远程终端服务等。若要防止远程使用此计算机，请清除“系统”属性控制面板项目的“远程”选项卡上的复选框	自动	手动
Terminal Services Configuration	该服务允许管理员使用远程桌面或远程管理设置，包括每会话临时文件夹、TS 主题和 TS 证书	手动	手动
Terminal Services UserMode Port Redirector	支持远程连接的打印机、驱动器、端口重定向功能，如果不希望使用远程功能，则可以关闭该服务	手动	手动
Themes	为用户提供使用主题管理的经验，如 Aero 功能	禁用	禁用
Thread Ordering Server	提供特别的线程排序和调度服务	手动	手动
TPM Base Services	允许访问受信任的平台模块，该模块向系统组件和应用程序提供基于硬件的加密服务。如果关闭该服务，应用程序将无法使用 TPM 保护的密钥	自动（延迟启动）	手动

续表

服务名称	功　能	默认状态	推荐设置
UPnP Device Host	这是系统中通用即插即用的设备的宿主程序，是此类设备和操作系统通信的主体，如果停止此服务，则所有宿主的 UPnP 设备都将停止工作，并且不能添加其他宿主设备	禁用	禁用
User Profile Service	该服务是装载和卸载用户配置文件。如果关闭该服务，用户将无法成功登录或注销，应用程序可能无法获得用户数据	自动	自动
Virtual Disk	提供用于磁盘、卷、文件系统和存储阵列的管理服务	手动	手动
Volume Shadow Copy	该服务用于管理并执行用于备份和其他目的的卷影复制。如果关闭该服务，则将无法使用卷影复制功能，并且备份会失败	手动	手动
Windows Audio	管理基于 Windows 系统的音频程序。如果关闭该服务，音频设备和效果将不能正常工作	手动	手动
Windows Audio Endpoint Builder	管理 Windows 音频服务的音频设备。如果此服务被停止，音频设备和效果将不能正常工作	手动	手动
Windows Color System	Windows 系统色彩管理模块，如 Windows 颜色系统基线颜色设备和 gamut 映射模型的特定于供应商的扩展。如果关闭该服务，则可能导致颜色显示不正确	手动	手动
Windows Driver Foundation - User-mode Driver Framework	管理用户模式驱动的主进程，主要应用于程序开发人员	手动	手动
Windows Error Reporting Service	允许在程序停止运行或停止响应时报告错误，并提供现有解决方案。如果此服务被停止，则错误报告将无法正确运行，并且不显示诊断服务和修复的结果	自动	手动
Windows Event Collector	该服务主要为系统提供性能分析和系统监控功能，包括 Windows 事件日志、硬件以及启用 IPMI 的事件源。该服务将转发的事件存储在本地活动日志中，如果关闭，将无法创建事件订阅和接受转发的事件	手动	手动
Windows Event Log	此服务管理事件和事件日志，支持日志记录事件、查询事件、订阅事件、归档事件日志以及管理事件元数据。如果关闭该服务，则可能危及系统的安全性和可靠性，尤其是对服务器而言	自动	自动
Windows Firewall	该服务主要提供 Windows 防火墙功能，可以通过限制未授权用户或程序访问本地计算机来保护系统安全	自动	自动
Windows Installer	添加、修改和删除以 Windows Installer(*.msi)程序包提供的应用程序。如果禁用了此服务，将无法执行此类安装程序，任何完全依赖它的服务不会被启动	手动	手动
Windows Management Instrumentation	系统管理服务，为用户提供统一的界面和对象模式，以便访问有关操作系统、设备、应用程序和服务的管理信息。如果此服务被终止，多数基于 Windows 的软件将无法正常运行	自动	自动
Windows Modules Installer	启用 Windows 更新和可选组件的安装、修改和删除。如果此服务被禁用，则 Windows 更新的安装或卸载可能会失败	手动	手动

续表

服务名称	功　能	默认状态	推荐设置
Windows Remote Management (WS-Management)	允许从远程进行计算机管理或信息收集。WS-Management 是用于远程软件和硬件管理的标准 Web 服务协议。WinRM 服务侦听网络上的 WS-Management 请求并对它们进行处理	自动(延迟启动)	自动(延迟启动)
Windows Time	维护在网络上的所有客户端和服务器的时间和日期同步。如果此服务被停止，时间和日期的同步将不可用。如果关闭该服务，则域环境中的客户端可能无法登录到域控制器	自动	自动
Windows Update	启用检测、下载和安装 Windows 和其他程序的更新。如果此服务被禁用，这台计算机的用户将无法使用 Windows Update 或其自动更新功能，建议为服务器启用该服务	自动(延迟启动)	自动
WinHTTP Web Proxy Auto-Discovery Service	允许 HTTP 客户端自动发现代理服务器配置，该服务使应用程序支持 WPAD 协议的应用	手动	手动
Wired AutoConfig	此服务要求系统对以太网接口自动执行 IEEE 802.1X 身份验证	手动	手动
WMI Performance Adapter	WMI 信息转换，为性能监控、事件日志工具提供服务	手动	手动
Workstation	创建和管理到远程服务器的网络连接，在局域网环境中，必须启用该服务才可以实现与其他计算机的连接	自动	手动

2.6 端口安全

端口，是服务器上的网络服务得以对外提供的主要通道，一台被配置 IP 地址的服务器，可以提供多种不同的网络服务，这主要是因为每个网络服务使用的端口是不同的。每个 IP 地址可提供 65536 个端口，有些端口是默认开放的，有些则是关闭的，而开放的端口随时都有可能成为非法入侵者的跳板，因此，必须充分了解计算机的端口开放情况。

2.6.1 端口分类

通常情况下，IP 地址的端口都是以端口号来标记的，端口号是从 0～65535 之间的一个任意整数。从逻辑意义上说，端口分类有多种分类标准，按端口号分布划分和按协议类型划分是其中较为常用的两种分类方法。

1. 端口号划分

按照端口号划分，可以将端口分为 3 大类，即公认端口、注册端口、动态或私有端口。

(1) 公认端口

公认端口(Well Known Ports)范围为 0～1023。这些端口号一般被系统固定的分配给一些服务。例如：21 端口被分配给 FTP 服务；25 端口被分配给 SMTP(简单邮件传输协议)服务；110 端口被分配给 POP3 服务；80 端口被分配给 WWW 服务；135 端口被分配给 RPC(远程过程调用)服务等。

(2) 注册端口

注册端口(Registered Ports)范围为 1024～49151。注册端口松散绑定于一些服务，即端口号一般都不会固定的分配给某个服务，许多服务都可以使用这些端口。只要运行的程序向系统提出访问网络的申请，那么，系统就可以从这些端口号中，自动分配一个端口给程序使用。比如，1024 端口就是分配给第一个向系统发出申请的程序，而在该程序进程关闭后，就会释放其所占用的 1024 端口。因此，注册端口在一定程度上降低了系统的安全性。

(3) 动态或私有端口

动态或私有端口(Dynamic or Private Ports)范围为 49512～65535。通常情况下，不建议为服务分配这些端口。动态端口和注册端口并无太大区别，因此也可以直接将端口按照端口号划分为公认端口(0～1023)和私有端口(1024～65535)。

2. 协议类型划分

端口按协议类型划分，可以分为 TCP、UDP 等端口。

(1) TCP 端口

TCP 端口是由 TCP 协议而来的，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。

常用 TCP 端口包括以下内容。

- HTTP：超文本传送协议使用 80 端口，用于实现 Web 服务和网页浏览。
- FTP：文件传输协议使用 21 端口，用于实现文件的上传和下载。
- SMTP：简单邮件传送协议使用 25 端口，用于发送电子邮件。
- POP3：邮局协议使用 110 端口，用于接收电子邮件。

(2) UDP 端口

UDP 端口，即用户数据包协议端口，无需在客户端和服务器之间建立连接，安全性得不到保障。常见的有 DNS 服务的 53 端口，SNMP(简单网络管理协议)服务的 161 端口，QQ 使用的 8000 和 4000 端口等。

常用 UDP 端口包括以下内容。

- DNS：域名解析服务使用 53 端口。用于实现将域名解析为 IP 地址。


提示：DNS 服务还同时使用 TCP 53 端口。

- SNMP：简单网络管理协议使用 161 端口，用于实现对网络设备的远程管理和监视。由于网络设备很多，无连接的服务就体现出其优势。
- QQ：QQ 服务使用 8000 端口，侦听是否有信息发送过来，客户端使用的则是 4000 端口，并通过该端口向外发送信息。但如果上述端口正在使用(例如，同时与几个好友聊天)，则端口号顺序自动递增 4001、4002。

2.6.2 端口攻击

看似神秘的网络攻击其实很多都是通过端口实现的，默认情况下，系统为了提供各种网络服务和网络

访问功能，已经开放了许多端口，处于“待命”状态。入侵者通常都是借助于各种扫描工具，探测某用户计算机的端口开放情况，最终实施系统攻击的。植入木马是比较常用的端口攻击方式之一。简单地讲，木马就是未经用户许可就在计算机中安装的非法外联软件。

木马主要有以下两种方式：

- 开放服务端口的木马。这类木马都需要在使用者的计算机上开启某个服务端口作为“后门(BackDoor)”，成功后该后门处于 LISTENING 状态，其端口号可能固定一个数，也可能变化，还有的木马可以与正常的端口合用。例如开着正常的 80 端口(WWW 服务)，木马也用 80 端口。这种木马最大的特点就是有端口处于 LISTENING 状态，需要远程计算机连接它。这种木马对一般用户比较好防范，将防火墙设为拒绝从外到内的连接即可。比较难防范的是反弹型木马。
- 反弹型木马。反弹型木马是从内向外的连接，可以有效地穿透防火墙，即使使用的是内网 IP，一般也能访问使用者的计算机。这种木马的原理是服务端主动连接客户端(黑客)地址。木马的服务端软件就像 Internet Explorer 一样，使用动态分配端口去连接客户端的某一端口，通常是常用端口，像端口 80，而且会使用隐蔽性较强的文件名，例如 iexplore.exe、explorer(IE 的程序是 IEXPLORE.EXE)。

计算机病毒和木马通过端口和其他的计算机进行连接，在网络环境中，可以使用防火墙或者本地安全策略的方式关闭某些端口。

2.6.3 查看端口——netstat

根据系统提供正在运行应用程序和网络服务的不同，端口状态也可能是不断变化的，并且有些应用程序可能会同时调用多个端口，而端口的数量有几万个之多，要想了解当前端口的开放情况和工作状态并非易事。netstat 命令是 TCP/IP 协议簇中的一个常用命令，可以帮助用户查看本地系统端口的开放情况。

1. netstat 命令简介

netstat 主要用于显示活动的网络连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息(对于 IP、ICMP、TCP 和 UDP 协议)以及 IPv6 统计信息(对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议)等。如果不使用任何参数，则显示系统内的活动的 TCP 连接。

netstat 命令的语法格式：

```
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]
```

netstat 参数说明：

- -a——显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。
- -b——显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下显示包含于创建连接或监听端口的组件序列。这种情况下，可执行组件名在底部的[ ]中，顶部是其调用的组件。注意此选项可能需要很长时间，如果没有足够权限可能失败。
- -e——显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与-s 结合使用。
- -f——显示外部地址的完全限定域名(FQDN)。
- -n——显示活动的 TCP 连接，但只以数字形式表现地址和端口号，而不会确定其名称。
- -o——显示活动的 TCP 连接并包括每个连接的进程 ID(PID)。可以在 Windows 任务管理器中的“进

程”选项卡上，找到基于 PID 的应用程序。该参数可以与-a、-n 和-p 结合使用。

- -p Proto——显示 Protocol 所指定的协议的连接。在这种情况下，Protocol 可以是 TCP、UDP、TCPv6 或 UDPv6。如果该参数与-s 一起使用，按协议显示统计信息，则 Protocol 可以是 TCP、UDP、ICMP、IP、TCPv6、UDPv6、ICMPv6 或 IPv6。
- -r——显示 IP 路由表的内容。该参数与 route print 命令等价。
- -s——按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果系统还安装了 Windows XP 的 IPv6 协议，就会显示有关 IPv6 上的 TCP、IPv6 上的 UDP、ICMPv6 和 IPv6 协议的统计信息。可以使用-p 参数指定协议集。
- -t——显示当前连接卸载状态。
- Interval——每隔一定时间重新显示一次选定的信息，单位是秒。按 Ctrl+C 停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息。



注意：与该命令一起使用的参数必须以连字符(-)作为前缀，而不能是短斜线(/)作为前缀。

2. 查看当前连接

查看当前有哪些计算机正在与本机连接，并且所使用的 IP 地址以及端口等信息，如果想要达到这个目的，可以使用 netstat 命令行的方法。

单击“开始”按钮，在“开始搜索”文本框中，输入“cmd”并按 Enter 键，显示“命令提示符”窗口。在命令提示符下输入如下命令：

```
netstat -na
```

按 Enter 键执行命令，显示如图 2-36 所示的结果。

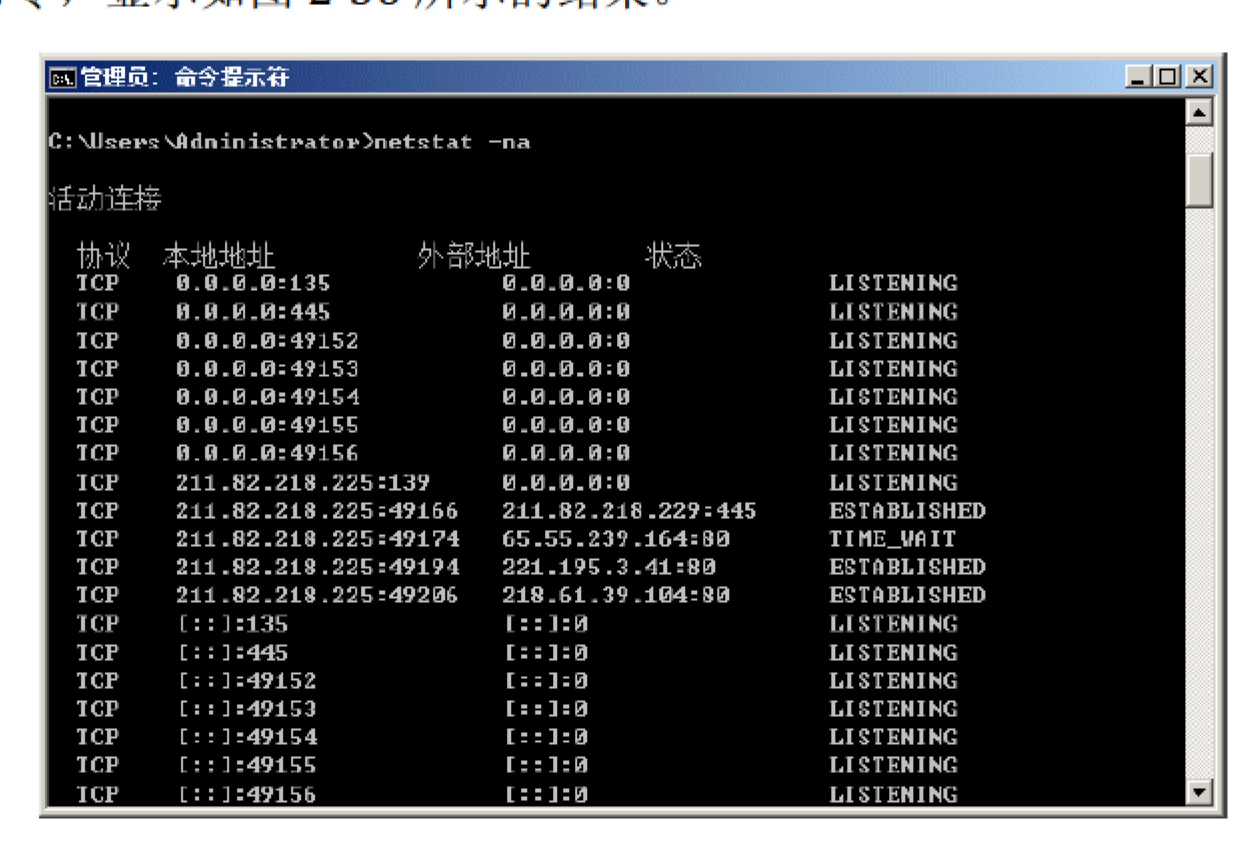


图 2-36　查看当前端口连接

命令执行结果显示本机连接情况及打开的端口。其中包括“协议”、“本地地址”、“外部地址”和“状态”等信息。“协议”表示通信协议的类型(TCP 或 UDP)。“本地地址”表示本地计算机的 IP 地址和正在使用的端口号。如果不指定-n 参数，则显示与 IP 地址和端口的名称对应的本地计算机名称。如果端口还没有建立的话，那么端口将以星号(*)显示。“外部地址”表示连接该端口的远程计算机的 IP 地址和端口号。如果不指定-n 参数，则显示与 IP 地址和端口对应的名称。如果端口还没有建立的话，那么端口

将以星号(*)显示。“状态”表示已建立连接的状态，通常包括 CLOSE_WAIT、CLOSED、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2、LAST_ACK、LISTENING、SYN_RECEIVED、SYN_SEND 和 TIMED_WAIT 几种类型。

3. 查看连接的宿主

所谓连接的宿主是指网络连接对应的应用程序或服务。通常情况下，仅凭开放端口是很难确认其安全与否的，发现可疑端口之后，首先要做的就是确认使用这些已经打开的端口的应用程序是哪个，然后进一步确认该程序是否为系统程序，如果不能确认，则可能是木马或其他非法程序。

在命令提示符窗口中，输入如下命令：

```
netstat -bn
```

按 Enter 键执行命令，显示如图 2-37 所示的结果。

```
管理员: 命令提示符
Microsoft Windows [版本 6.0.6001]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>netstat -bn

活动连接

  协议  本地地址              外部地址            状态
  TCP    211.82.218.225:49400   202.108.12.187:80      ESTABLISHED
 [iexplore.exe]
  TCP    211.82.218.225:49405   202.108.12.187:80      ESTABLISHED
 [iexplore.exe]
  TCP    211.82.218.225:49407   202.108.12.187:80      ESTABLISHED
 [iexplore.exe]
  TCP    211.82.218.225:49414   202.108.12.187:80      ESTABLISHED
 [iexplore.exe]

C:\Users\Administrator>
```

图 2-37　显示应用程序打开的端口

在命令执行结果中，显示了当前活动的每个连接都是由哪些程序创建的，本例中端口 49400、49405、49407 和 49414 都是由 iexplore.exe 程序打开的，均被用于访问外网的 Web 服务器。如果在结果中发现计算机打开了可疑的端口，就可以使用该命令查看它调用了哪些组件，然后再检查各组件的创建时间和修改时间，如果发现异常，就可能是中了木马。

2.6.4　通过组策略配置端口

通过运行端口查看工具，不难发现系统中的许多端口默认都是开启的，为了确保系统和网络的安全，必须将可能存在安全风险的端口及时关闭。在域环境中，管理员可以通过组策略对客户端计算机需要开放的端口进行筛选。这里以关闭 139 端口为例，详细描述在组策略编辑器中创建 IP 安全策略的步骤，分为以下几部分：

- 创建组织单位和策略。
- 创建 IP 筛选器。
- 创建 IP 筛选器操作。
- 创建 IP 安全规则。
- 创建 IP 安全策略。
- 指派 IP 安全策略。



注意：在 Windows 域环境下创建 IPSec 策略时，必须使用具有“组策略”管理权限的用户才可以完成。想要管理计算机本地或远程 IPSec 策略，必须是本地或远程计算机 Administrators 组的成员。

1. 创建新的组织单位和策略

IP 安全策略控制法主要是针对客户端系统而言的，因此实施之前，必须确保客户计算机已经加入域中，为了便于管理，建议将欲配置的客户统一添加到新建 OU 中。Windows Server 2008 中创建基于 OU 或域的组策略，与 Windows Server 2003 略有不同，所有的组策略配置都是在“组策略管理”控制台中完成的。

① 打开“Active Directory 用户和计算机”窗口，新建 OU 并将欲配置的客户计算机加入到该 OU，如图 2-38 所示。

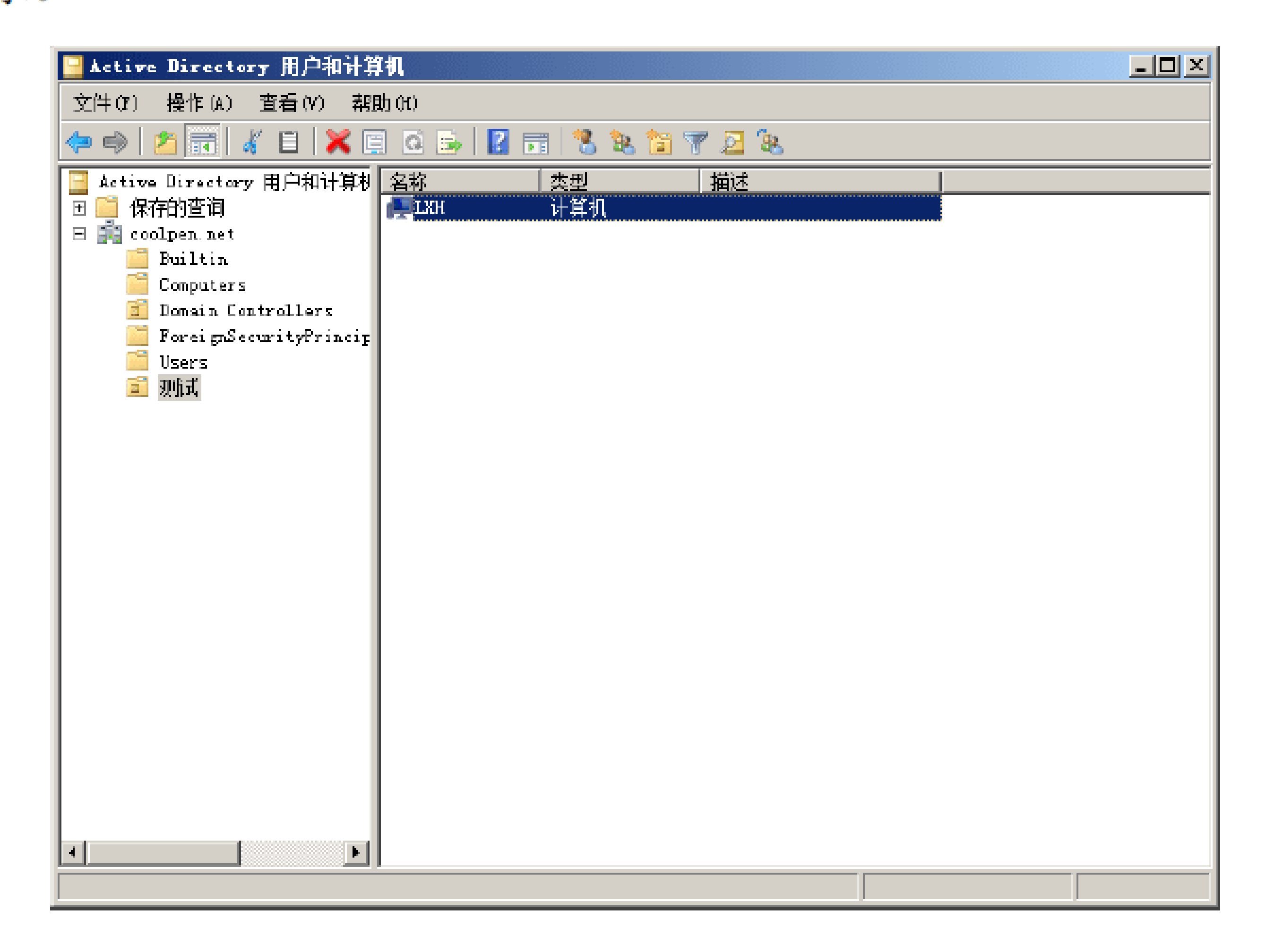


图 2-38　创建 OU

② 依次选择“开始”→“管理工具”→“组策略管理”选项，打开如图 2-39 所示的“组策略管理”控制台窗口。

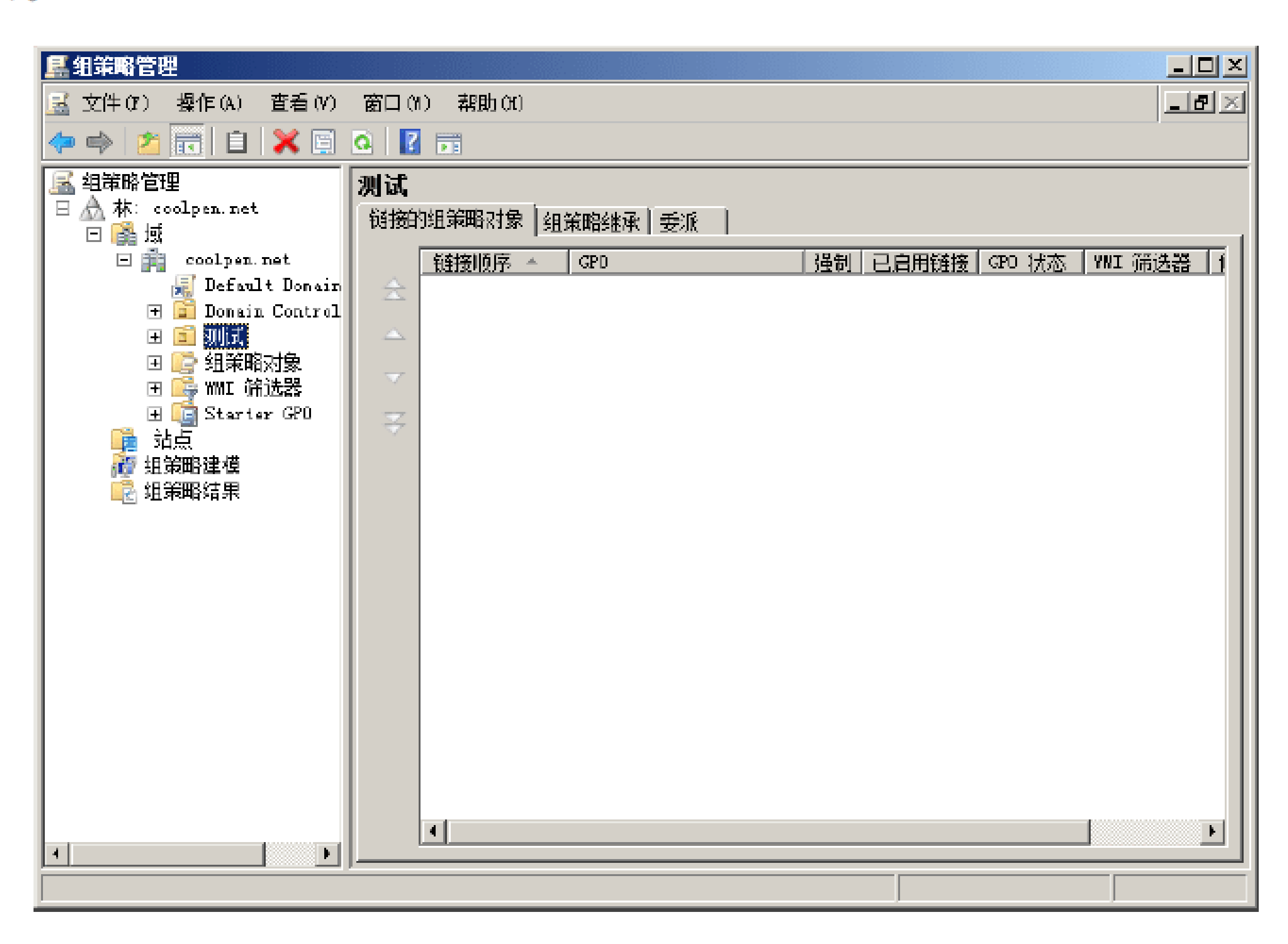


图 2-39　“组策略管理”窗口

③ 右击需要创建组策略的组织单位，选择快捷菜单中的“在这个域中创建 GPO 并在此处链接”命令，打开如图 2-40 所示的“新建 GPO”对话框，在“名称”文本框中输入新建 GPO 的名称。



图 2-40 “新建 GPO”对话框

④ 单击“确定”按钮，即可完成组策略的创建，如图 2-41 所示。

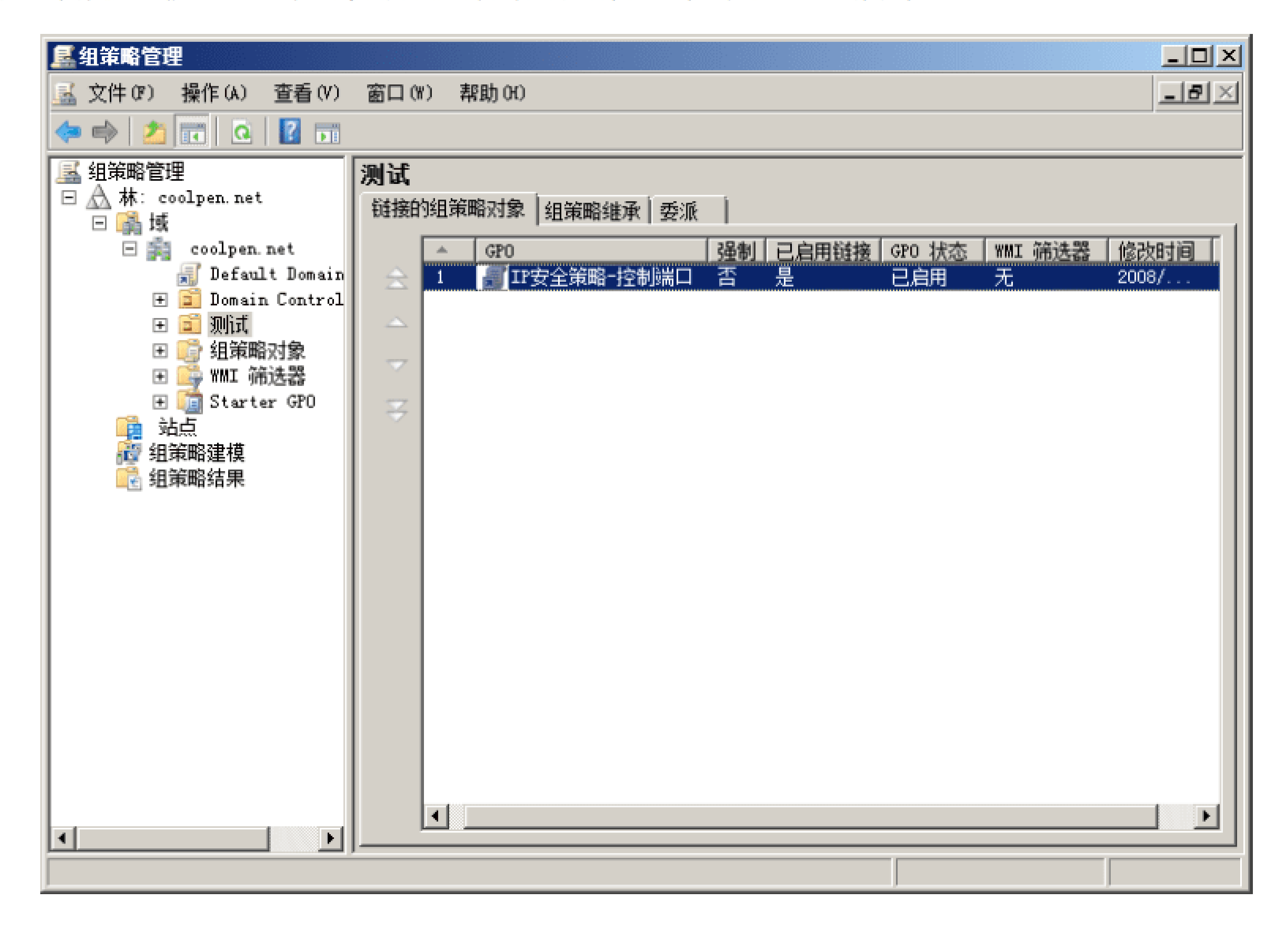


图 2-41 新创建的组策略

2. 定义 IP 筛选器

可以在创建策略时或者在创建策略之前定义筛选器列表，已经创建的筛选器列表可用于任何策略。每个筛选器定义入站或出站网络通信的子集，即筛选器操作通过保护通信(使用身份验证、数据完整性或数据加密)、完全阻止或允许(不使用身份验证、数据完整性或数据加密)的方式进行操作。

① 右击新创建的组策略“IP 安全策略-控制端口”，选择“编辑”，打开“组策略管理编辑器”窗口。依次展开“计算机配置”→“Windows 设置”→“安全设置”→“IP 安全策略，在 Active Directory(coolpen.net)”，如图 2-42 所示。

② 右击“IP 安全策略，在 Active Directory(coolpen.net)”，选择快捷菜单中的“管理 IP 筛选器表和筛选器操作”命令，打开如图 2-43 所示的“管理 IP 筛选器表和筛选器操作”对话框。

③ 在默认显示的“管理 IP 筛选器列表”选项卡中，单击“添加”按钮，显示如图 2-44 所示的“IP 筛选器列表”对话框。在“名称”文本框中，输入容易记忆的筛选器名称，便于与其他 IP 筛选器区别，如“TCP 139”。在“描述”文本框中，输入相关的描述信息，可以方便日后的应用和管理。

④ 单击“添加”按钮，打开“IP 筛选器向导”，显示如图 2-45 所示的“IP 筛选器向导”对话框。

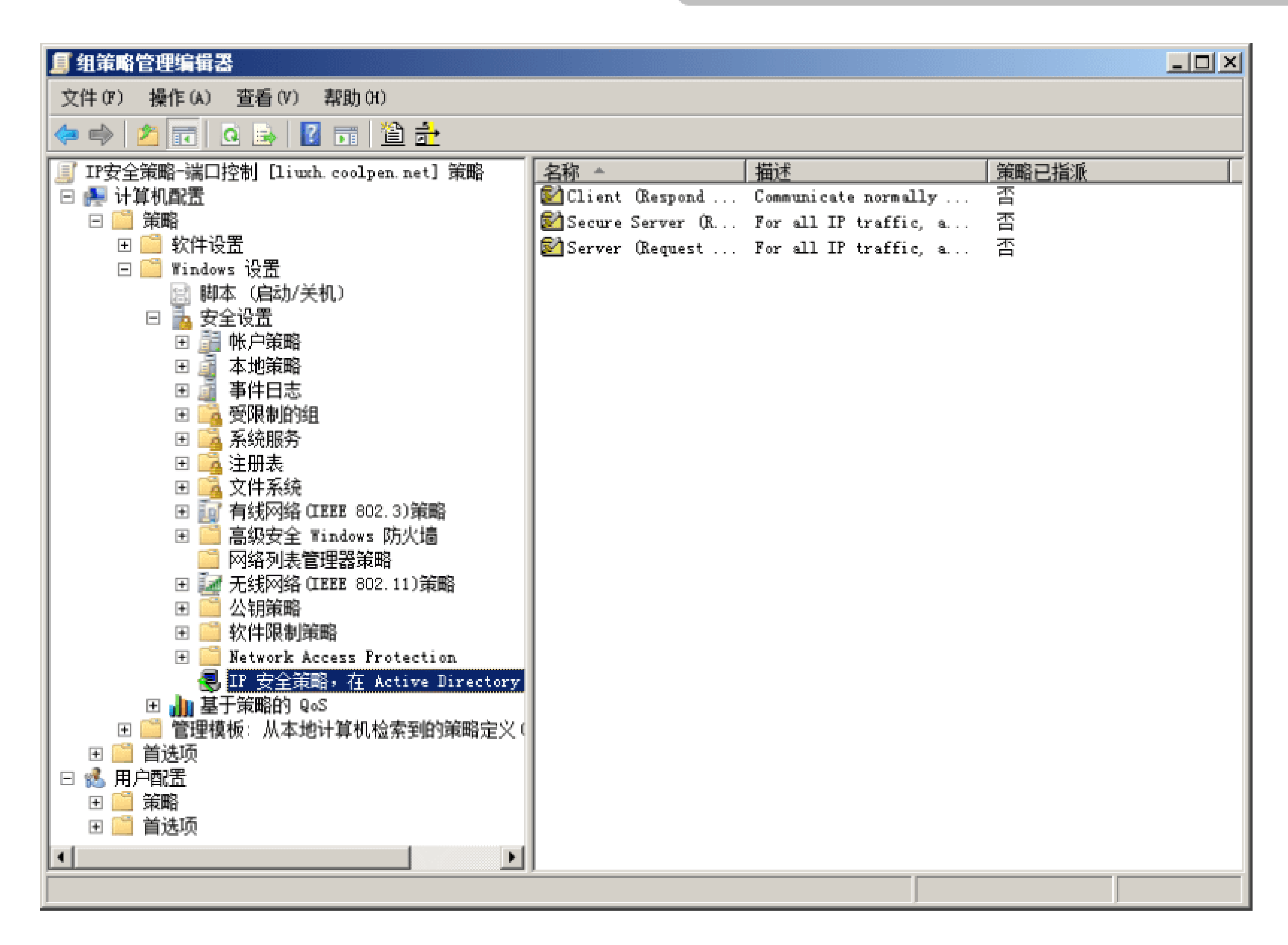


图 2-42　“组策略管理编辑器”窗口

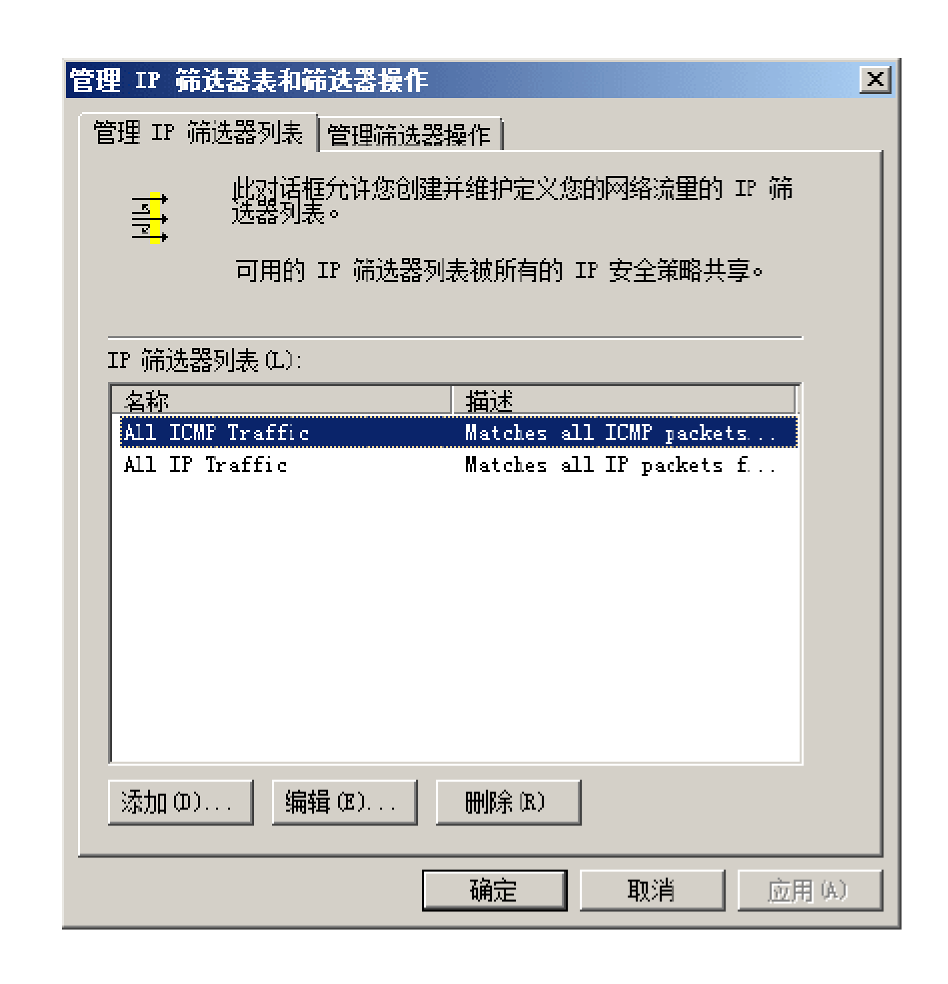


图 2-43　“管理 IP 筛选器表和筛选器操作”对话框

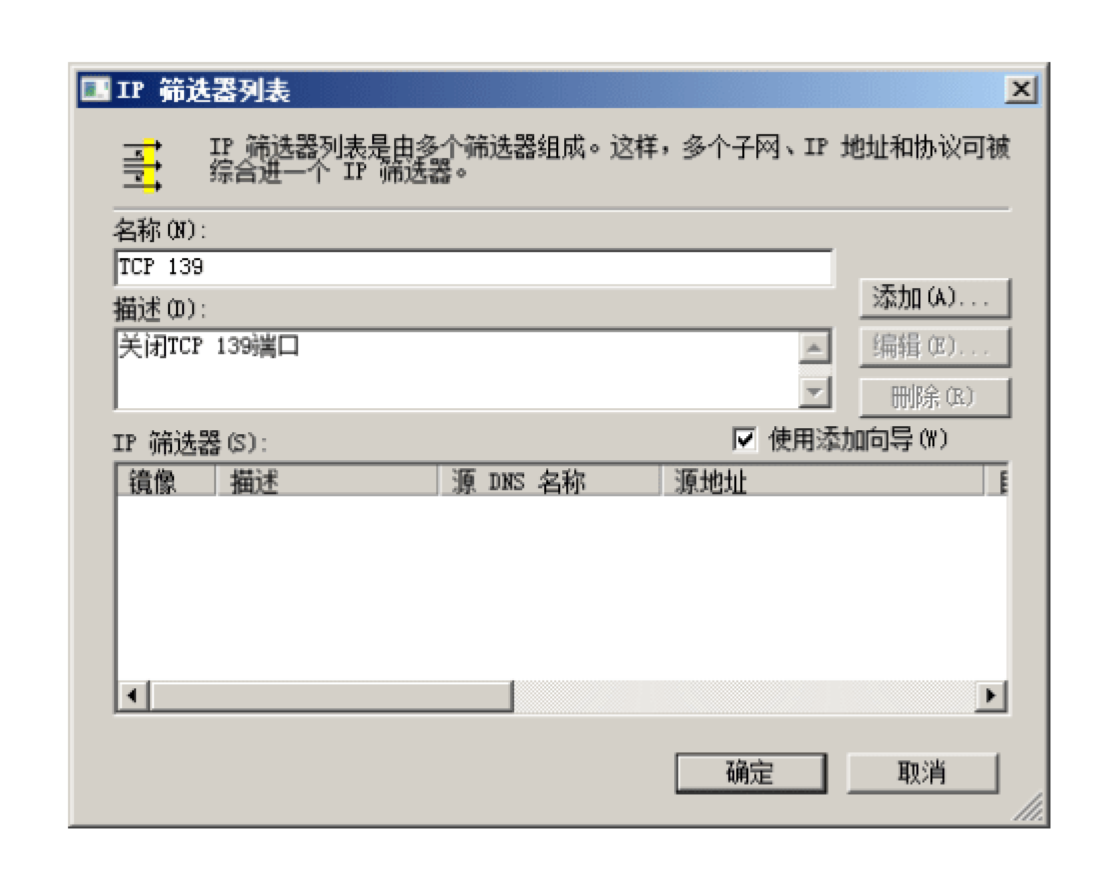


图 2-44　“IP 筛选器列表”对话框

⑤ 单击“下一步”按钮，显示如图 2-46 所示的“IP 筛选器描述和镜像属性”界面。默认情况下，已经选中“镜像”复选框，此时将根据筛选器设置自动创建两个筛选器，一个用于到目标的通信，一个用于来自目标的通信。如果取消选中“镜像”复选框，则将先创建基于筛选器设置的单一筛选器。



提示：在取消选中“镜像”复选框的情况下，进行隧道操作时，必须手动创建下面两个筛选器列表。其中，一个列表描述通过隧道发出的通信(出站通信)，另一个列表描述通过隧道接收的通信(入站通信)。然后，创建两个规则，这些规则使用策略中的入站与出站筛选器列表。

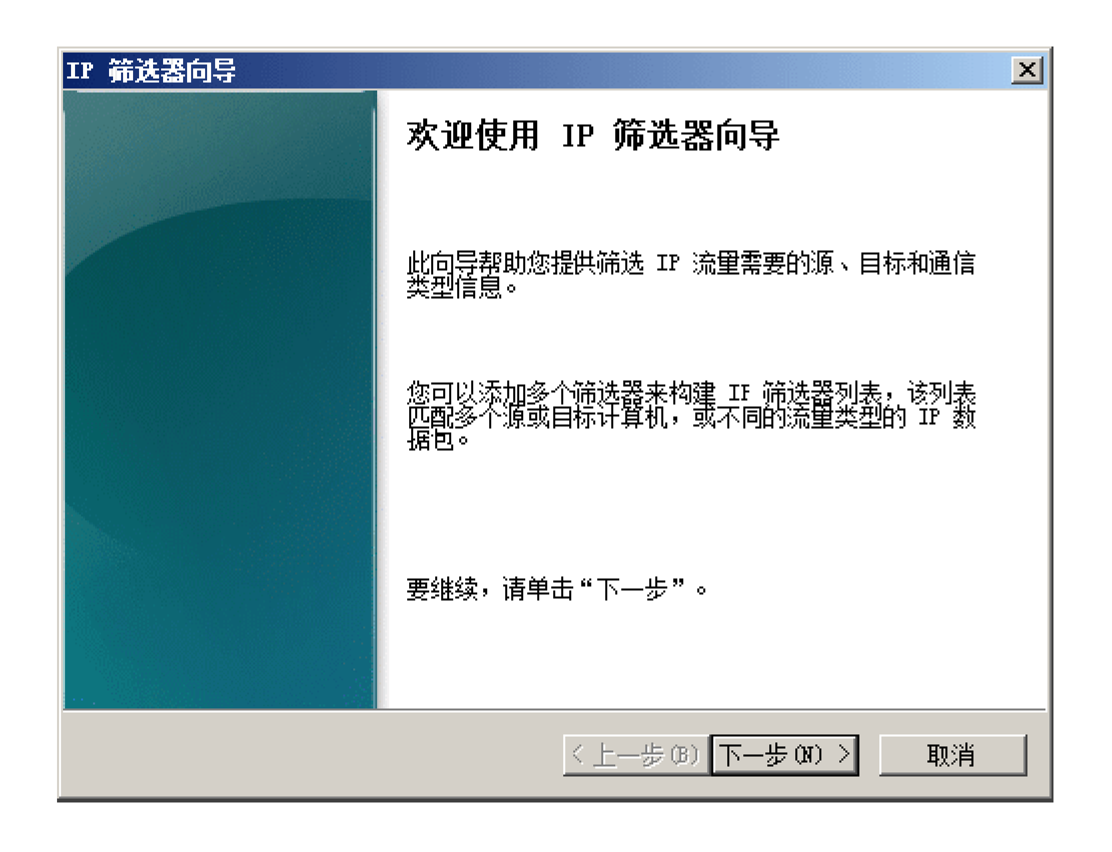


图 2-45 “IP 筛选器向导”对话框

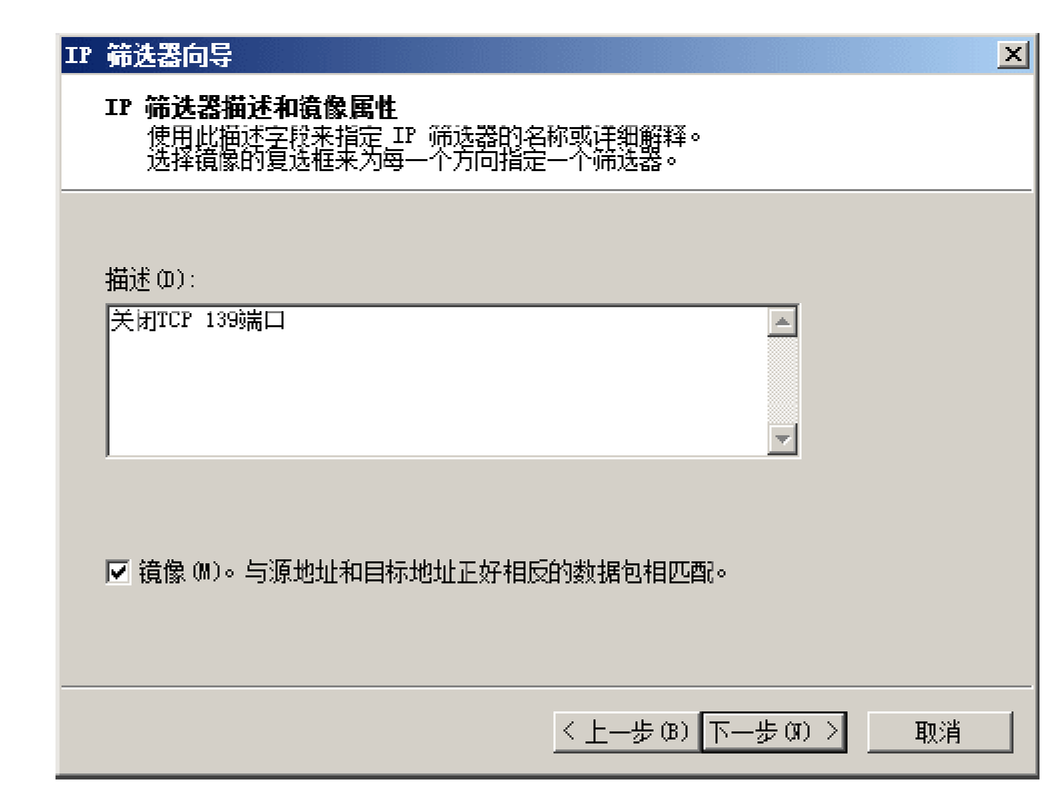


图 2-46 “IP 筛选器描述和镜像属性”界面

⑥ 单击“下一步”按钮，显示如图 2-47 所示的“IP 流量源”界面。在“源地址”下拉列表框中选择“任何 IP 地址”选项。“源地址”下拉列表中共包括“我的 IP 地址”、“任何 IP 地址”、“一个特定的 IP 地址或子网”、“DNS 服务器(动态)”、“WINS 服务器(动态)”、“DHCP 服务器(动态)和默认网关(动态)”等选项。

⑦ 单击“下一步”按钮，显示如图 2-48 所示的“IP 流量目标”界面，在“目标地址”下拉列表框中选择“我的 IP 地址”选项。

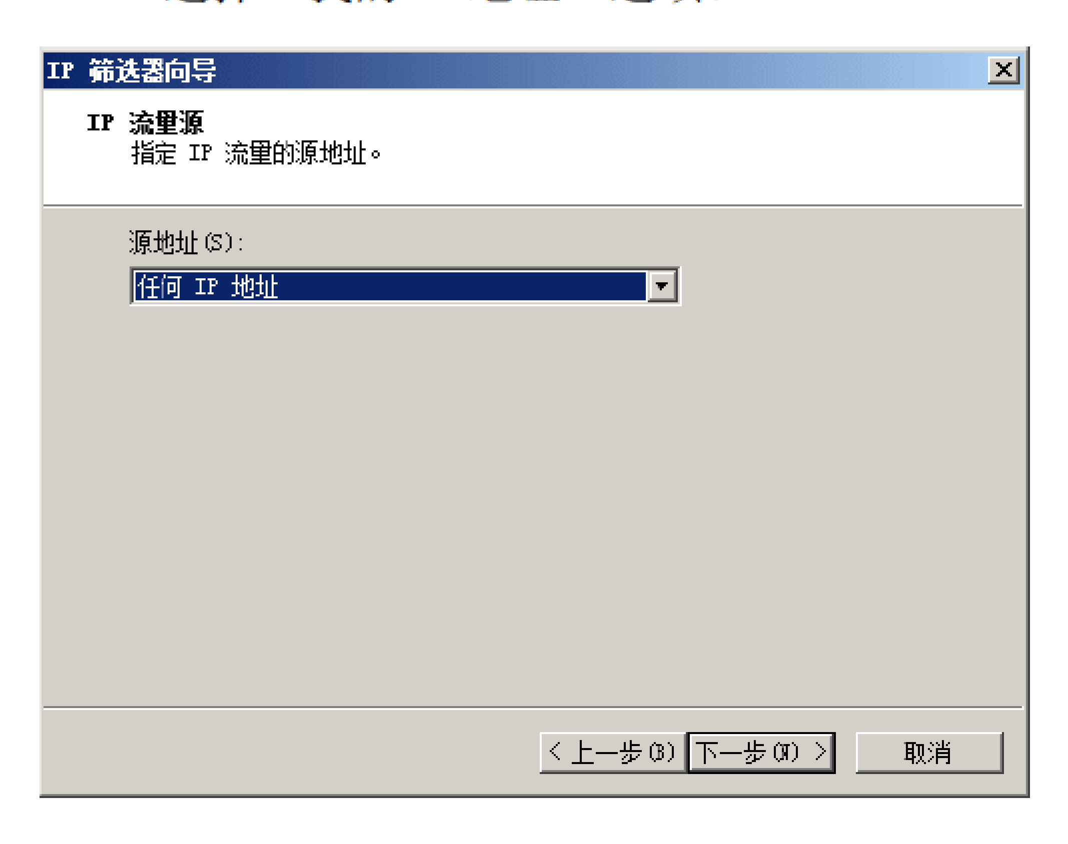


图 2-47 “IP 流量源”界面

图 2-48 “IP 流量目标”界面

⑧ 单击“下一步”按钮，显示如图 2-49 所示的“IP 协议类型”界面，在“选择协议类型”下拉列表框中，选择 TCP 选项。

“选择协议类型”的策略如下：

- 如果选择 TCP 或 UDP，则还可以通过目标端口筛选数据包。
- 如果要筛选从选定协议类型所用的任意端口上发送的数据包，可选择“从任意端口”选项。
- 如果要筛选从选定协议类型所用的特定端口上发送的数据包，可选择“从此端口”选项，然后输入端口号。
- 如果要筛选从选定协议类型所用的任意端口上接收的数据包，可选择“到任意端口”选项。
- 如果只筛选在指定的端口号上接收的数据包，可选择“到此端口”项。

注意：对于 IPSec 隧道，只支持基于地址的筛选器，而不支持特定协议和特定端口的筛选器。

⑨　单击“下一步”按钮，显示如图 2-50 所示的“IP 协议端口”界面，分别选择“从任意端口”和“到此端口”单选按钮，并在“到此端口”文本框中输入端口号“139”。



图 2-49　“IP 协议类型”界面

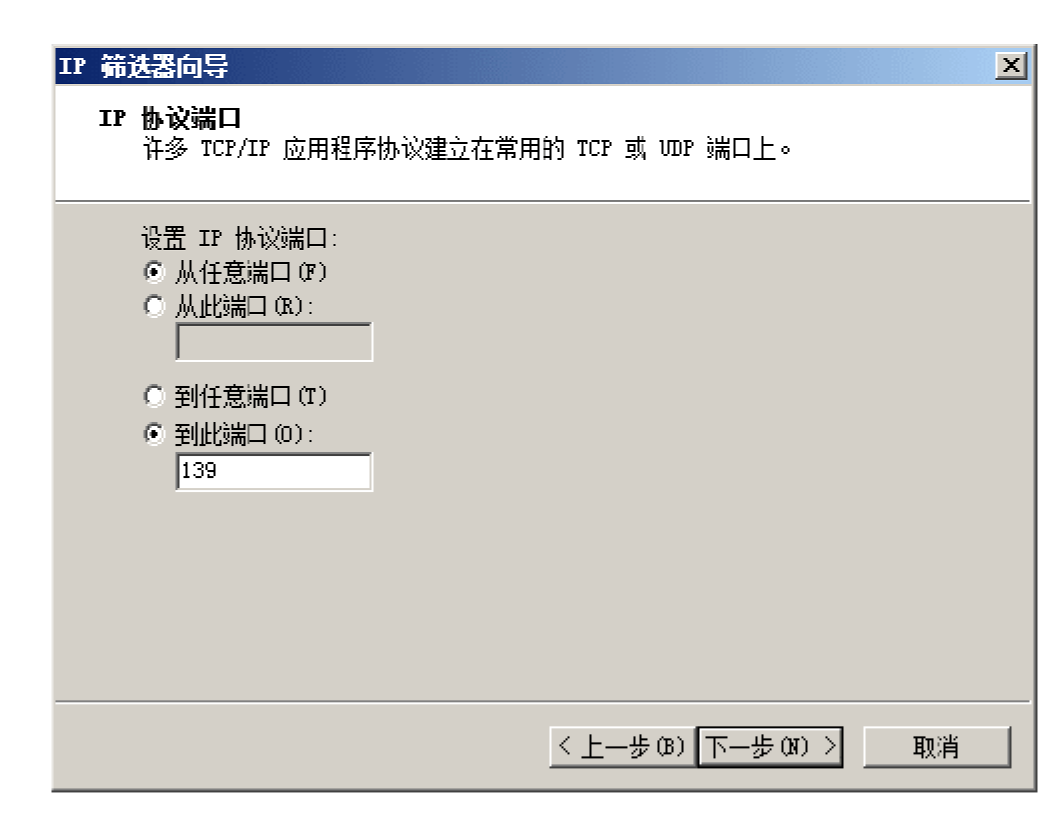


图 2-50　“IP 协议端口”界面

⑩　单击“下一步”按钮，显示如图 2-51 所示的“正在完成 IP 筛选器向导”界面，如果同时选中“编辑属性”复选框，则单击“完成”按钮后即可立即编辑该 IP 筛选器。

⑪　单击“完成”按钮，显示如图 2-52 所示的“IP 筛选器列表”对话框，新创建的筛选器已经显示在列表中。

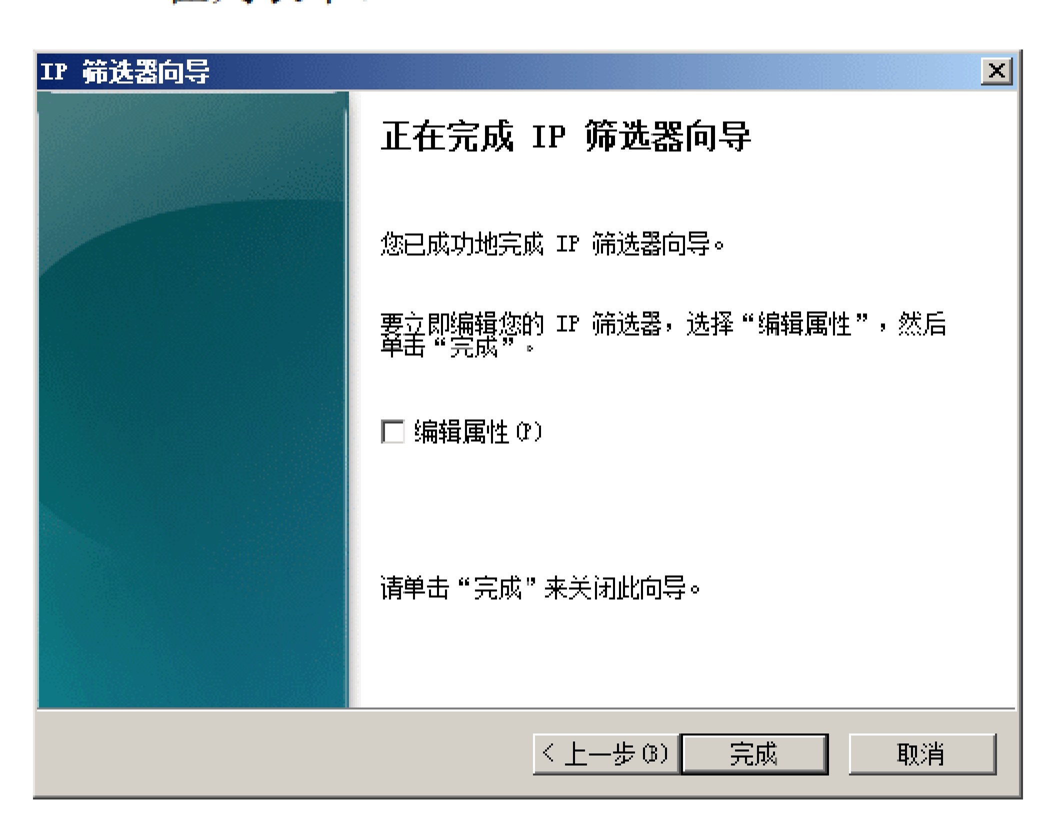




图 2-51　“正在完成 IP 筛选器向导”界面

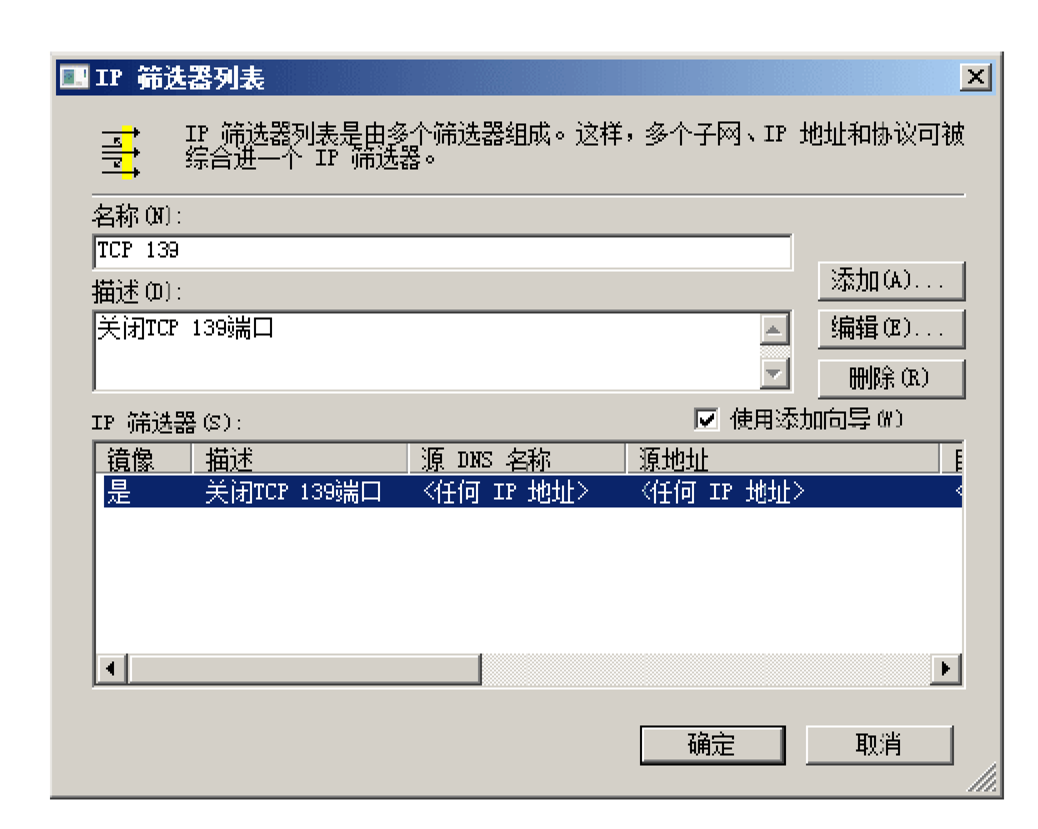


图 2-52　成功创建的 IP 筛选器

注意：对于受 IPSec 策略保护的计算机而言，筛选器是 IP 安全策略的重要组成部分。如果不在客户机或服务器策略中指定适当的筛选器，或者如果在更新该策略的筛选器之前 IP 地址已经更改，则可能无法提供安全保护。另外，建议不要在 IPSec 筛选器中使用 DHCP 分配的 IP 地址。对于由使用 DHCP 地址的计算机所使用的策略，应使用“我的 IP 地址”作为源地址或目标地址。这样，即使计算机 IP 地址更改，系统也会自动更新“我的 IP 地址”筛选器。最后，在 IPSec 保护通信的计算机策略中，确保目标计算机的筛选器目标地址是静态 IP 地址，所有目标 IP 地址必须包含在筛选器列表中。

将新的静态 IP 地址添加到受安全策略保护的计算机中时：

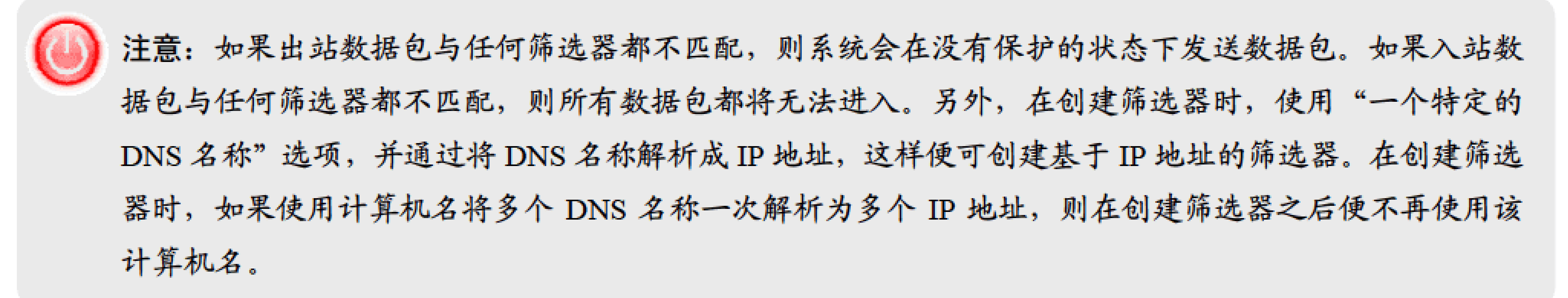
- 应修改对受保护的计算机进行安全保护的所有客户机和服务器上的 IPSec 策略筛选器，在添加新地址之前，应确保这些客户机已经更新其策略。
- 检查将在受保护的计算机上使用的策略。如果筛选器为本地连接指定静态 IP 地址，则在向其接口添加新的 IP 地址后，应编辑并保存新的筛选器列表，并保证新的静态 IP 地址包含在其中。需要注意的是，在添加新的静态 IP 地址时，“我的 IP 地址”筛选器将自动更新，而不用用户再进行手动更新。

如果受保护的计算机是 WWW 服务器，并且客户机使用的是代理服务器，则应确保网络上所有的通信都受 IPSec 保护：

- WWW 服务器和所有直接连接的客户端之间的通信。
- WWW 服务器和代理服务器之间的通信。
- 代理服务器及其所有客户机之间的通信。

下列的筛选器，被默认设置为允许(不保护)通信：

- Internet 密钥交换(IKE)。源地址=任意，目标地址=任意，协议=UDP，源端口=500，目标端口=500。
- IP 多播通信。
- IP 广播通信。
- KerberosV5。源地址=任意，目标地址=任意，协议=UDP 或 TCP，源端口=88，目标端口=88。
- 资源保留协议(RSVP)源地址=任意，目标地址=任意，协议=46。



注意： 如果出站数据包与任何筛选器都不匹配，则系统会在没有保护的状态下发送数据包。如果入站数据包与任何筛选器都不匹配，则所有数据包都将无法进入。另外，在创建筛选器时，使用“一个特定的 DNS 名称”选项，并通过将 DNS 名称解析成 IP 地址，这样便可创建基于 IP 地址的筛选器。在创建筛选器时，如果使用计算机名将多个 DNS 名称一次解析为多个 IP 地址，则在创建筛选器之后便不再使用该计算机名。

3. 定义 IP 筛选器操作

筛选器操作主要用于定义数据传输的安全需求，即对于符合筛选器条件的传输进行哪些处理，放行、阻止还是协商安全等。

① 在“管理 IP 筛选器表和筛选器操作”对话框中，切换至如图 2-53 所示的“管理筛选器操作”选项卡。

② 单击“添加”按钮，启动“筛选器操作向导”，显示如图 2-54 所示的“筛选器操作向导”对话框。

③ 单击“下一步”按钮，显示如图 2-55 所示的“筛选器操作名称”界面。在“名称”文本框中输入“拒绝访问 139 端口”。在“描述”文本框中，输入该筛选器的描述，例如这里输入“拒绝访问 139 端口”。

④ 单击“下一步”按钮，显示如图 2-56 所示的“筛选器操作常规选项”界面，这里定义 IPSec 策略的目的是关闭 139 端口，即拒绝其他主机对本地系统 139 端口的访问，所以应选择“阻止”单选按钮。

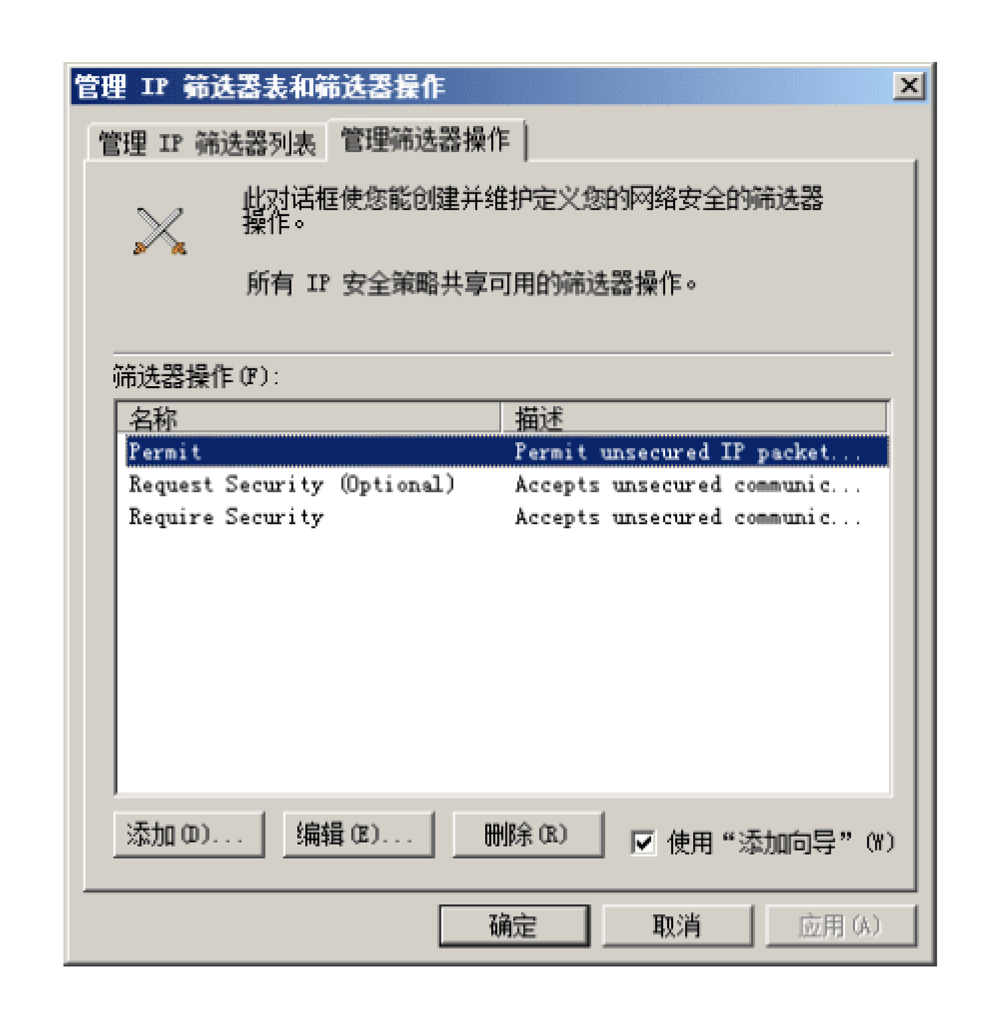


图 2-53　“管理筛选器操作”选项卡

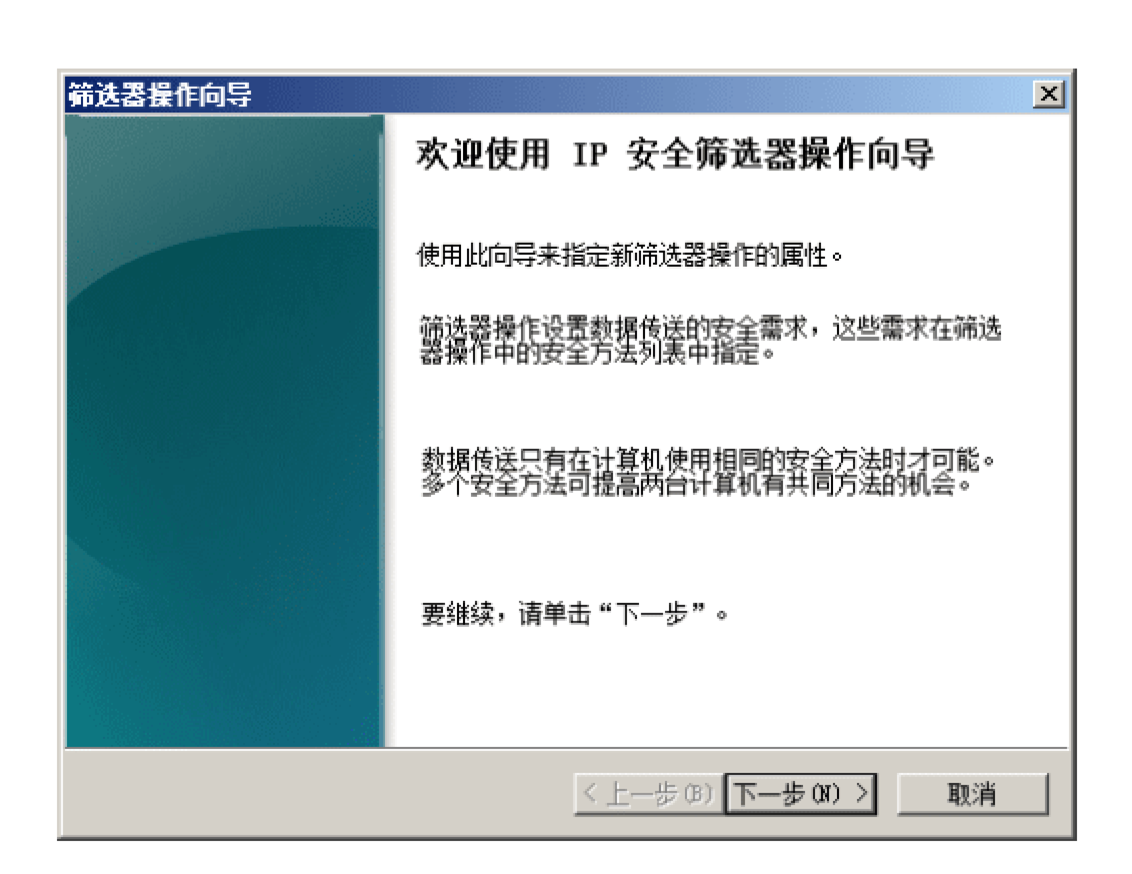


图 2-54　“筛选器操作向导”对话框

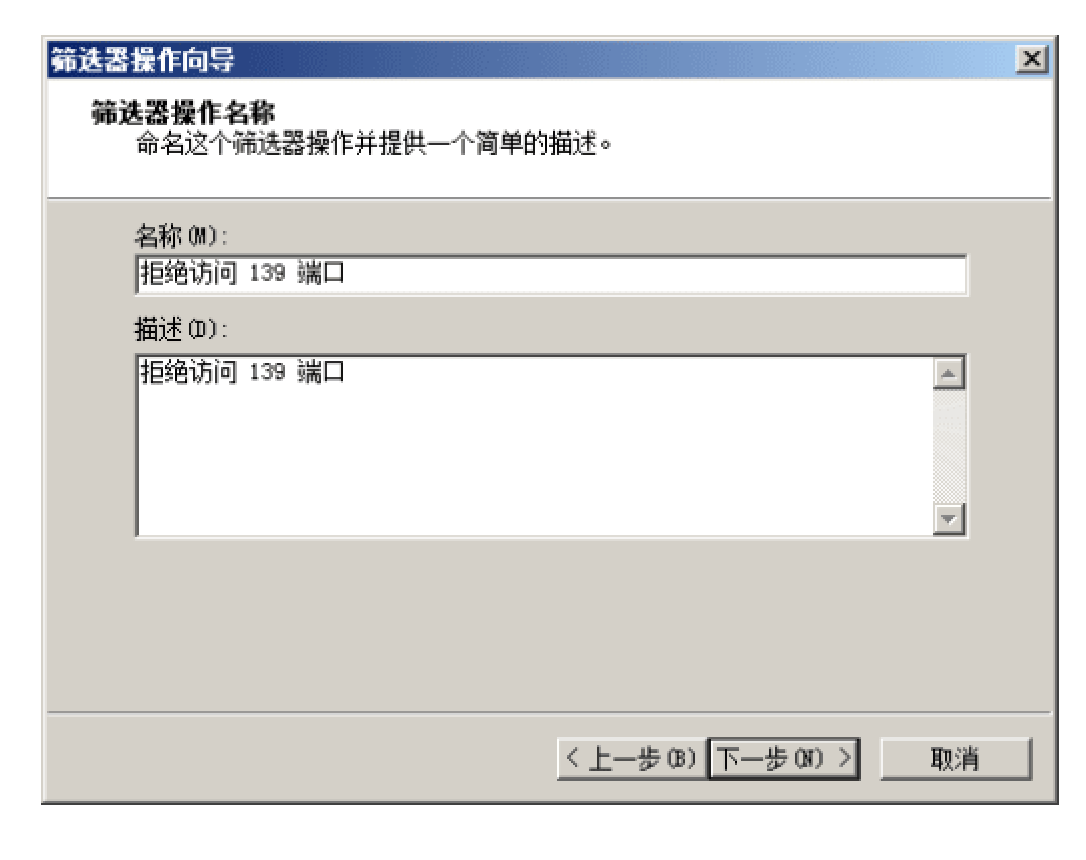


图 2-55　“筛选器操作名称”界面



图 2-56　“筛选器操作常规选项”界面

筛选器操作类型具体内容如下。

- 许可：允许以纯文本方式接收或发送数据包，不要求对这些数据包提供安全保护措施。
- 阻止：丢弃数据包。不要求对这些数据包提供安全措施。
- 协商安全：可使用“安全措施首选顺序”中的安全措施列表为数据包提供安全性，这些数据包的安全请求将被接受。

⑤ 单击“下一步”按钮，显示如图 2-57 所示的“正在完成 IP 安全筛选器操作向导”界面。选中“编辑属性”复选框并单击“完成”按钮，则可以立即编辑该筛选器操作。

⑥ 单击“完成”按钮，即可完成筛选器操作的创建。另外，如果不希望完全阻止来自其他主机的 139 端口访问，即希望允许与其他不支持 IPSec 的计算机通信，则可以在“管理 IP 筛选器表和筛选器操作”对话框的“管理筛选器操作”选项卡中，选择刚刚创建的“拒绝访问 139 端口”筛选器操作，并单击“编辑”按钮，打开如图 2-58 所示的“拒绝访问 139 端口 属性”对话框。选择“协商安全”单选按钮，并根据需要选择合适的协商条件即可。

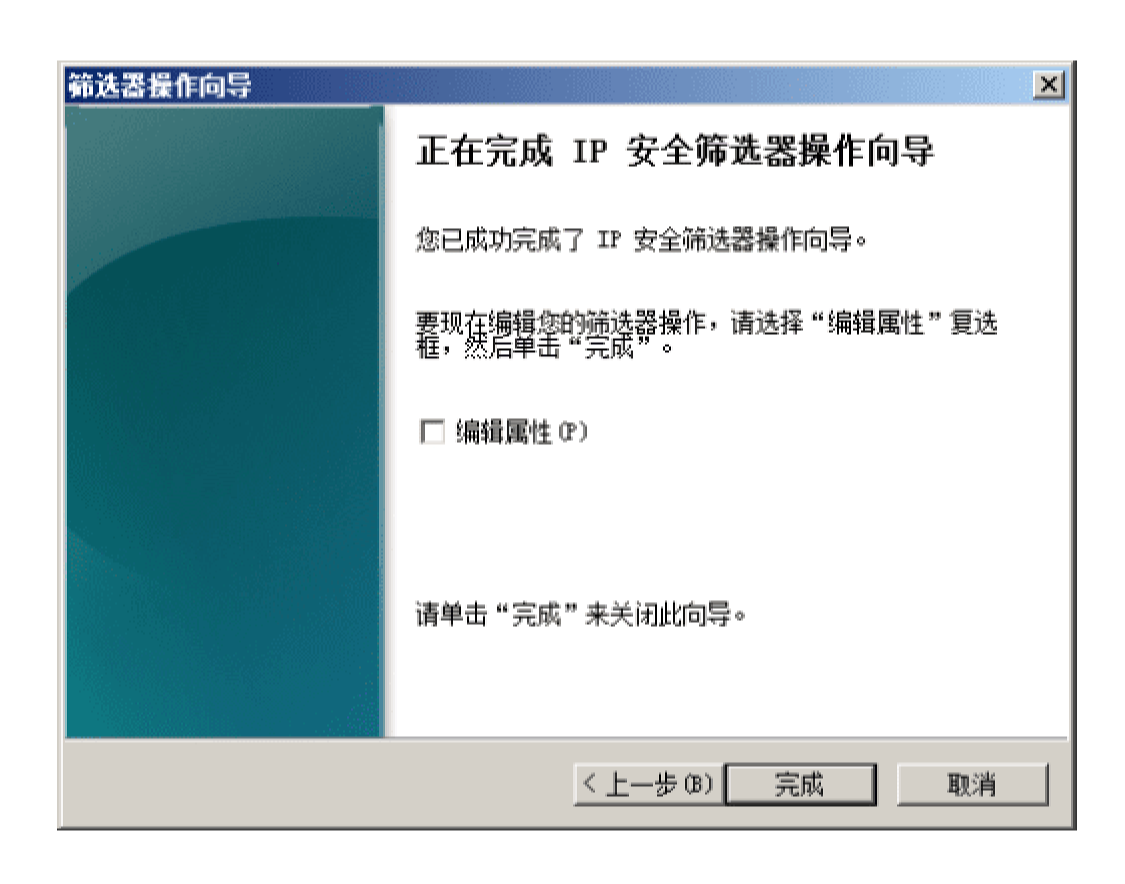


图 2-57 “正在完成 IP 安全筛选器操作向导”界面

图 2-58 “拒绝访问 139 端口 属性”对话框

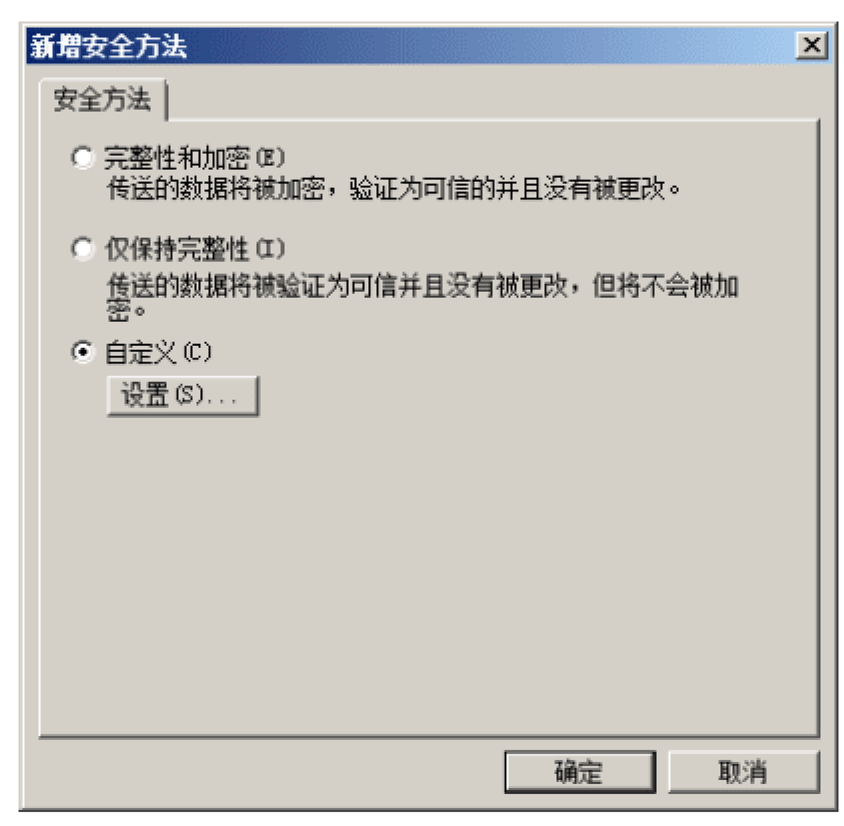
- 接受不安全的通讯，但始终用 IPSec 响应。IPSec 允许与不安全(未受 IPSec 保护)配置的筛选器列表相匹配的传入数据包。但是，必须对传入数据包的传出响应提供保护。将默认响应规则用于客户端时，该设置十分有用。将一组服务器用以下规则进行配置：该规则能够保护与任何 IP 地址的通信并能接受不安全通信，同时只用安全通信进行响应，并在客户端计算机上启用默认响应规则以确保客户端能够响应服务器的协商安全请求。若要阻止拒绝服务攻击，应当对连接到 Internet 的安全计算机禁用此选项。
- 如果无法建立安全连接，则允许回退到不安全的通信。如有必要，IPSec 将回退到不安全的通信。应当再次将 IP 筛选器列表限制在更小范围内。否则，当协商失败时，运用该筛选器的规则将会使不安全连接发送数据。如果环境对通信安全要求不高，则可以考虑禁用该设置。然而，这样可能会阻止与无法启动 IPSec 保护计算机的通信。若要阻止拒绝服务攻击，应当对连接到 Internet 的安全计算机禁用此选项。
- 使用会话密钥完全向前保密(PFS)。启用会话密钥 PFS 可以确保无法使用主密钥密钥资料以派生多个会话密钥。启用会话密钥 PFS 时，会执行新的 Diffie-Hellman(一种公开密钥交换算法)密钥交换，以便在创建新的会话密钥前生成新的主密钥材料。会话密钥 PFS 不需要重新进行主模式身份验证，并且使用的资源比主密钥 PFS 更少。

⑦ 在“安全方法首选顺序”列表中，可以设置筛选操作使用方法的先后顺序，默认是空白的。通常情况下，应当按照从最高安全性到最低安全性的顺序排列列表中的方法，这样可使用最安全的方法。单击“添加”按钮，打开如图 2-59 所示的“新增安全方法”对话框。

可供用户选择的安全方法包括如下内容。

- 完整性和加密。使用 ESP 协议可提供具有“三重数据加密标准(3DES)”算法的数据加密、具有“安全散列算法 1(SHA1)”完整性算法的数据完整性和身份验证，以及默认密钥寿命(100 MB，1 h)。
- 仅保持完整性。使用 ESP 协议可以提供数据完整性和身份验证(具有 SHA1 完整性算法)与默认密钥寿命(100 MB，1 h)。配置 ESP 不提供数据加密。
- 自定义。单击“设置”可配置自定义安全措施或密钥寿命。

⑧ 选择“自定义”单选按钮并单击“设置”按钮，显示如图 2-60 所示的“自定义安全方法设置”对话框。



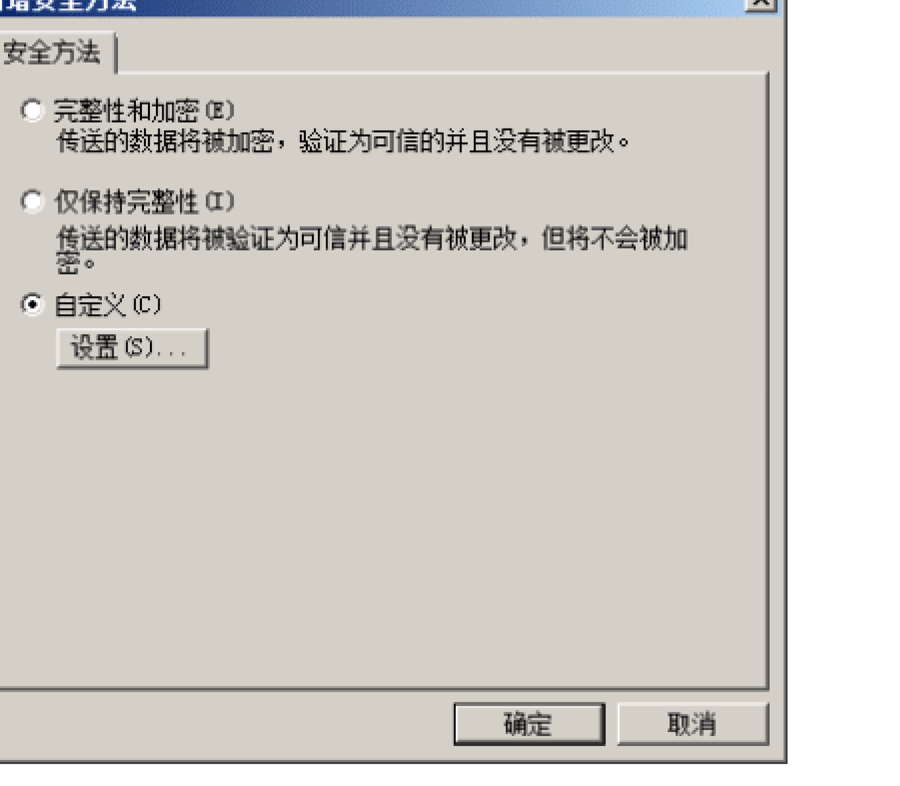


图 2-59　“新增安全方法”对话框

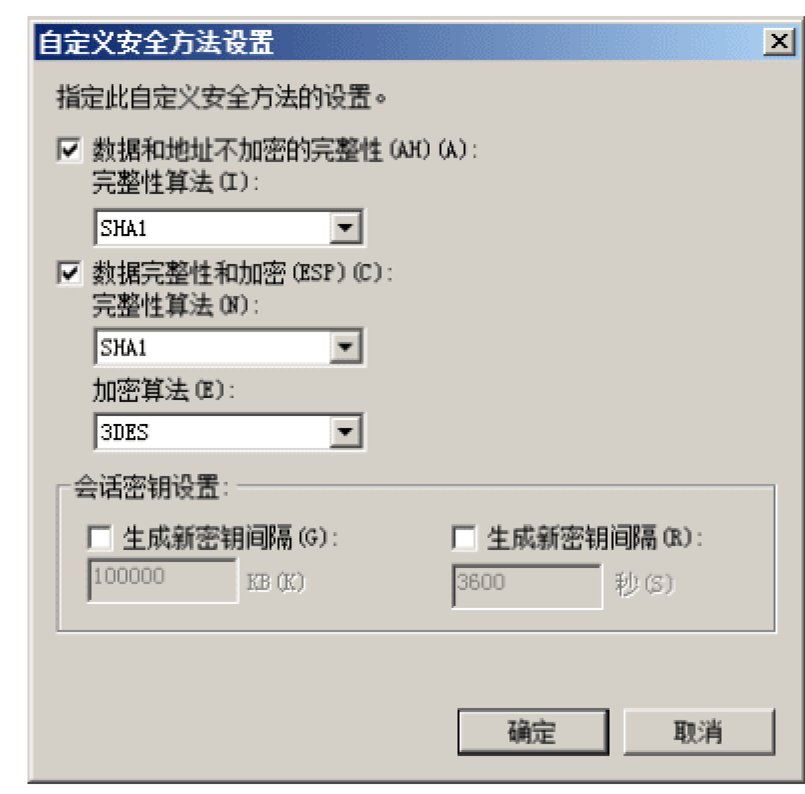


图 2-60　“自定义安全方法设置”对话框

若想要保障数据包寻址信息(IP 报头)和数据的完整性，可选中“数据和地址不加密的完整性(AH)”复选框。然后，在“完整性算法”下拉列表中，选择要用于数据完整性的算法。其中，各种加密算法的具体含义如下。

- MD5：使用“消息摘要 5(MD5)”完整性算法，该算法使用的是 128 位的密钥。
- SHA1：使用“安全散列算法 1”完整性算法，该算法使用的是 160 位的密钥。

要为数据提供完整性和加密(保密性)，选择“数据完整性和加密(ESP)”复选框，此时还应在“完整性算法”下拉列表中，选择数据完整性算法和加密算法。其中，各种完整性验证算法的具体含义如下。

- <无>：不使用数据完整性。如果已启用了“AH”，则可选择 ESP 完整性算法的“无”，以提高计算机的各项性能。
- MD5：使用 MD5 完整性算法，该算法使用的是 128 位的密钥。
- SHA1：使用 SHA1 完整性算法，该算法使用的是 160 位的密钥。

配合使用的各种加密算法的具体含义如下。

- <无>：不使用加密。
- DES：使用 56 位密钥的“数据加密标准(DES)”。
- 3DES：使用 3 个 56 位密钥的三重“数据加密标准”。

⑨ 连续单击“确定”按钮，保存设置即可。其实，第 6 步之后的操作都是为实现与未受安全策略保护的计算机的通信而设置的，管理员可以根据实际需要选择设置。

4. 创建 IP 安全策略

做好上述准备工作之后，即可开始创建 IP 安全策略。

① 在“组策略管理编辑器”窗口中，右击“IP 安全策略，在 Active Directory(coolpen.net)”选项，选择快捷菜单中的“创建 IP 安全策略”选项启动“IP 安全策略向导”，显示如图 2-61 所示的“IP 安全策略向导”对话框。

② 单击“下一步”按钮，显示如图 2-62 所示的“IP 安全策略名称”界面，在“名称”和“描述”文本框中，分别输入便于区分的策略名称，如“拒绝访问 139 端口”等。

③ 单击“下一步”按钮，显示如图 2-63 所示的“安全通讯请求”界面，保持系统默认设置即可。“激

活默认响应规则(仅限于 Windows 的早期版本)(R)”复选框仅对较早版本的 Windows 系统有效，对于 Windows Vista/2008 系统无效。

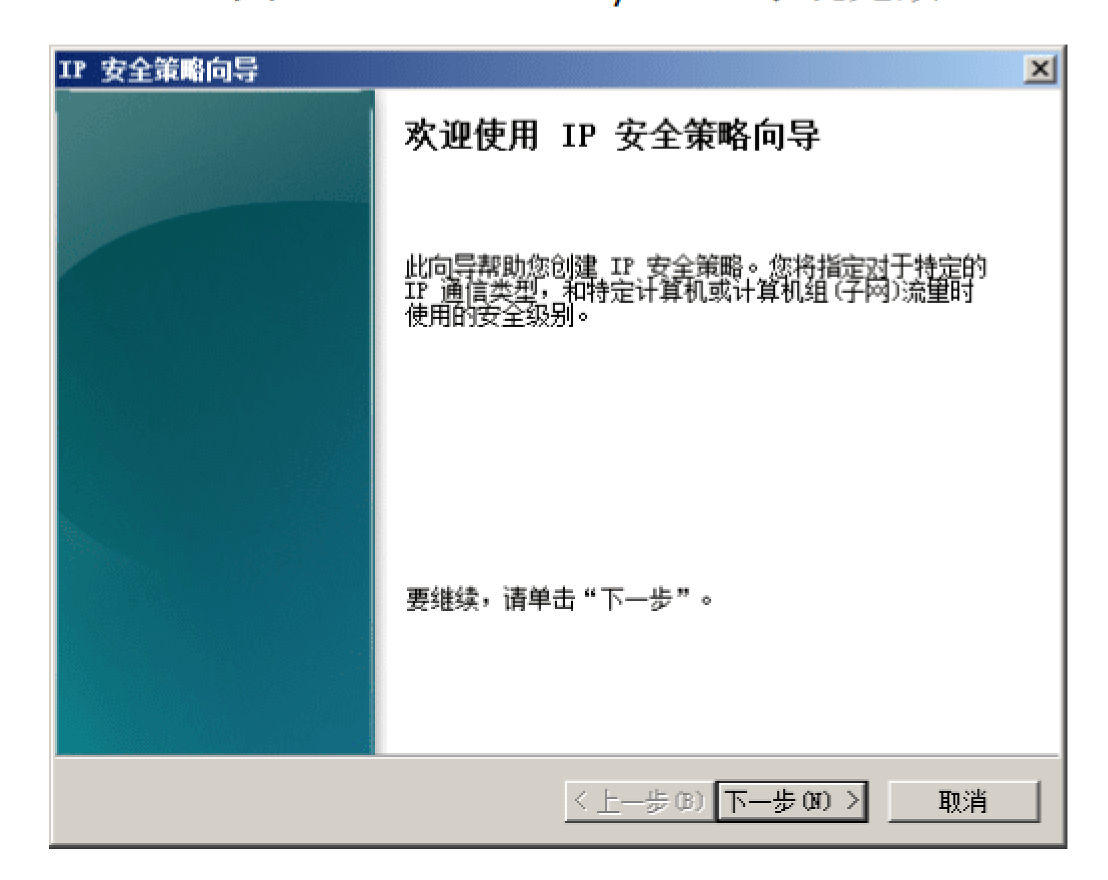


图 2-61 “IP 安全策略向导”对话框

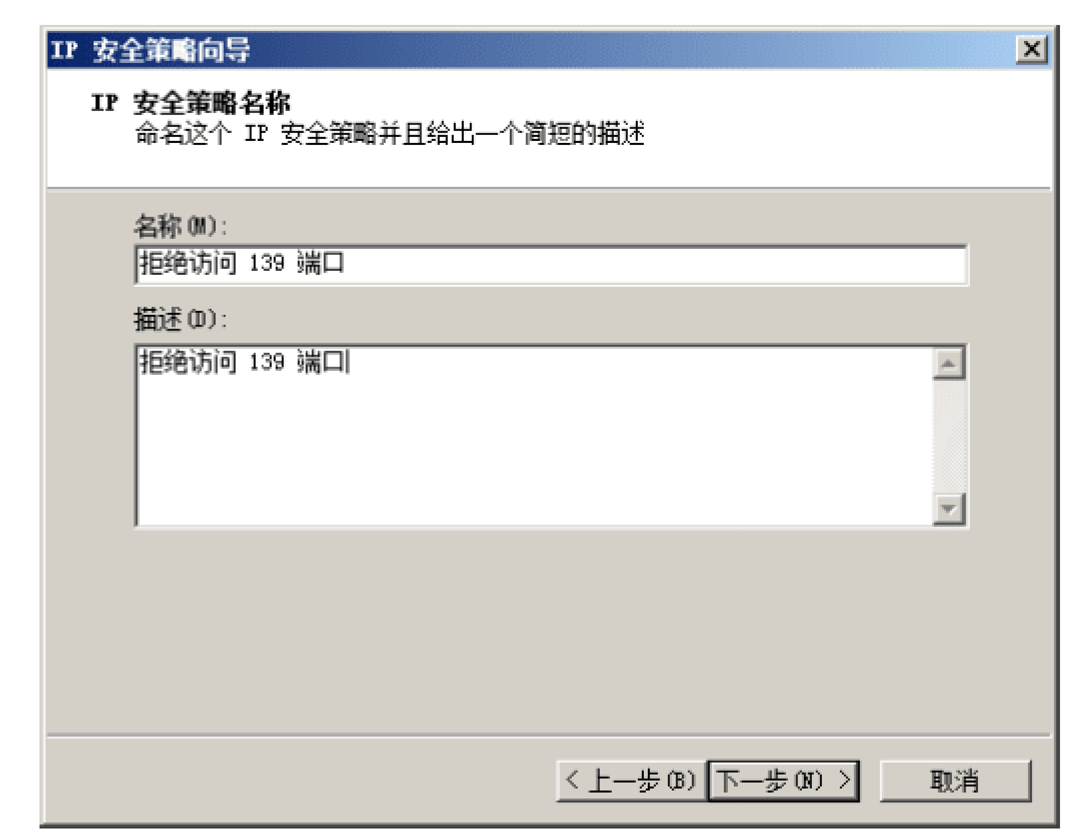


图 2-62 “IP 安全策略名称”界面

④ 单击“下一步”按钮，显示如图 2-64 所示的“正在完成 IP 安全策略向导”界面，取消“编辑属性”复选框，具体的策略属性将在“设置 IP 安全规则”中完成。

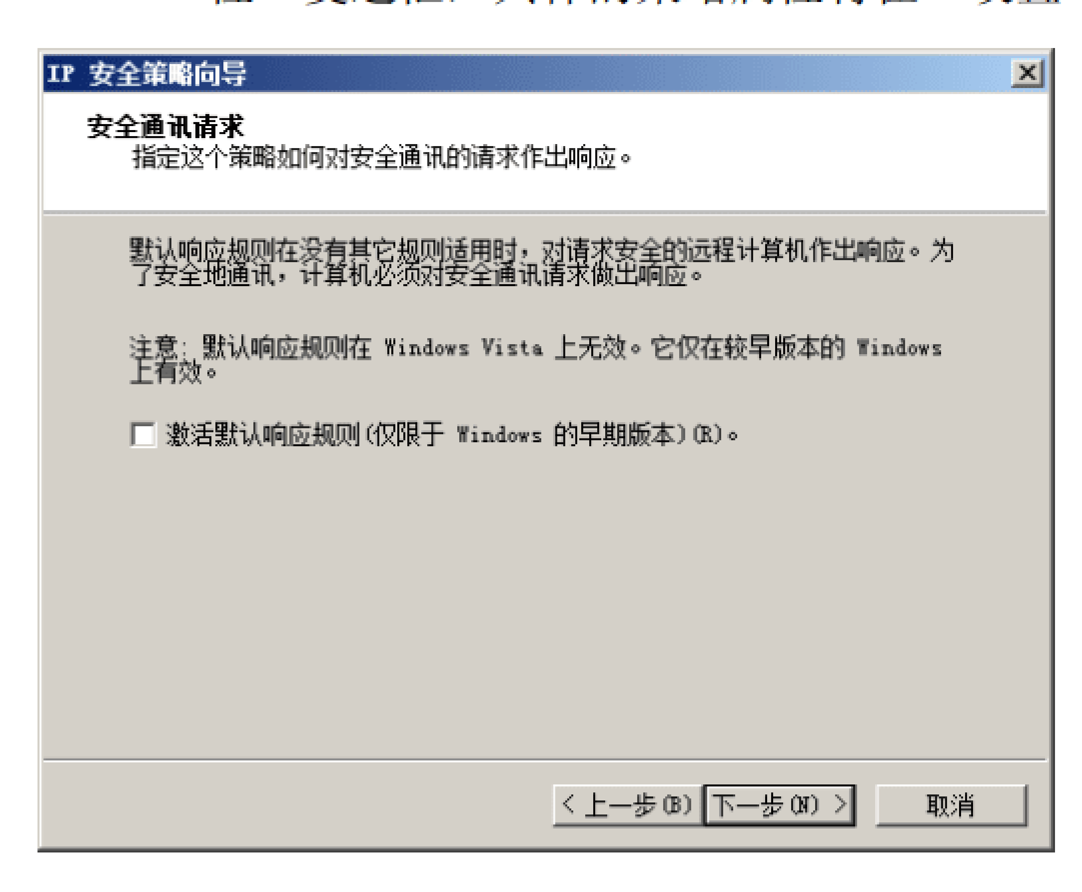


图 2-63 “安全通讯请求”界面

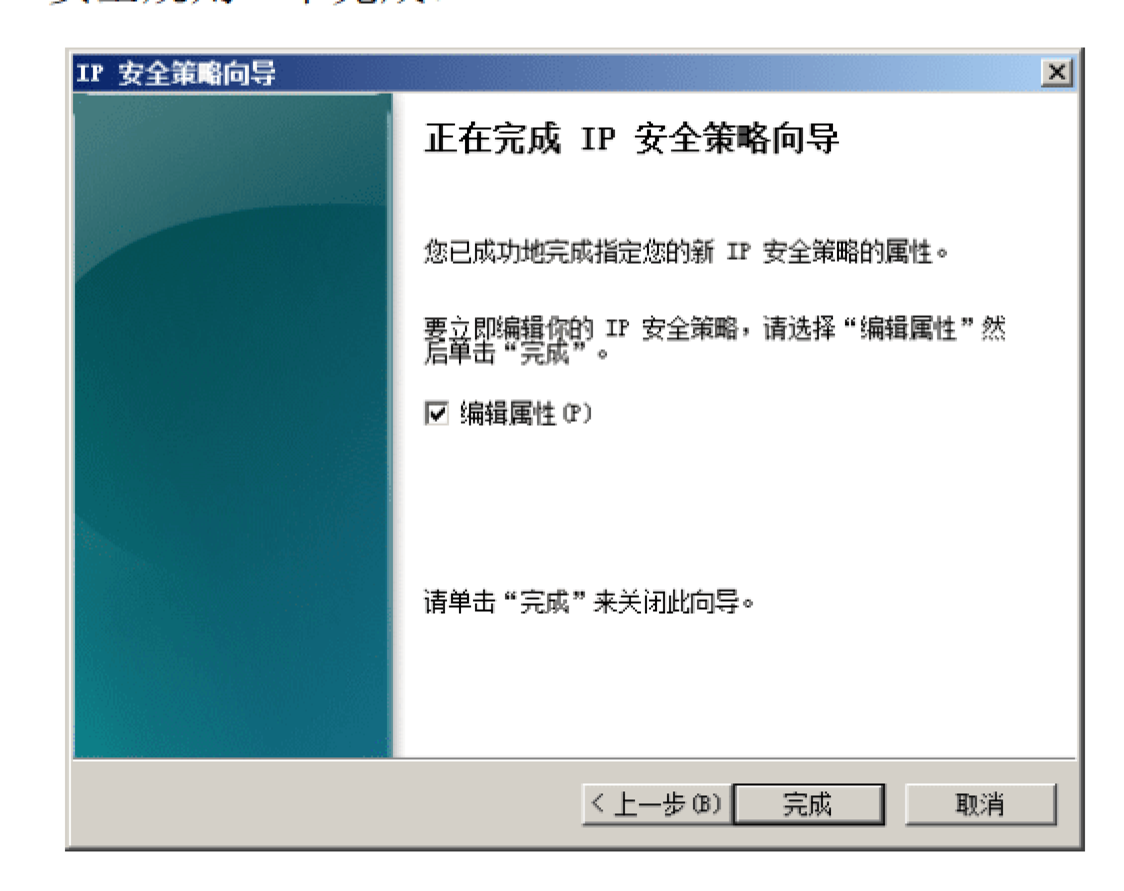


图 2-64 “正在完成 IP 安全策略向导”界面

⑤ 单击“完成”按钮，关闭“IP 安全策略向导”对话框，创建完成的“IP 安全策略”显示在“组策略管理编辑器”窗口中。

5. 设置 IP 安全规则

管理员在设置 IP 安全规则时，应注意以下事项：

■ 要定义基于 Active Directory 的 IPSec 策略，必须具有“组策略”管理权限。要管理计算机的本地或远程 IPSec 策略，必须是本地或远程计算机 Administrators 组的成员。

■ 成功添加的新规则将自动应用于正在创建或编辑的策略。在“IP 安全策略”中，策略规则基于为每一条规则选择的筛选器列表的名称以相反的字母顺序显示。需要注意的是，目前还没有方法能够指定应用于策略中规则的顺序。IPSec 会根据从最具体的筛选器列表到最不具体的筛选器列表进

行自动排序。

■ 自动在每个新的 IPSec 策略中，添加(并在选择后激活)默认响应规则。如果不希望此规则成为的策略的一部分，可通过取消“动态”复选框停用该规则，默认响应规则不能删除。

① 在“组策略管理编辑器”窗口中，双击需要设置安全规则的 IP 安全策略，显示如图 2-65 所示的“拒绝访问 139 端口　属性”对话框。

② 单击“添加”按钮，打开“安全规则向导”，显示如图 2-66 所示的“安全规则向导”对话框。将要设置的安全操作包括 IP 隧道操作属性、身份验证方法和筛选器操作。

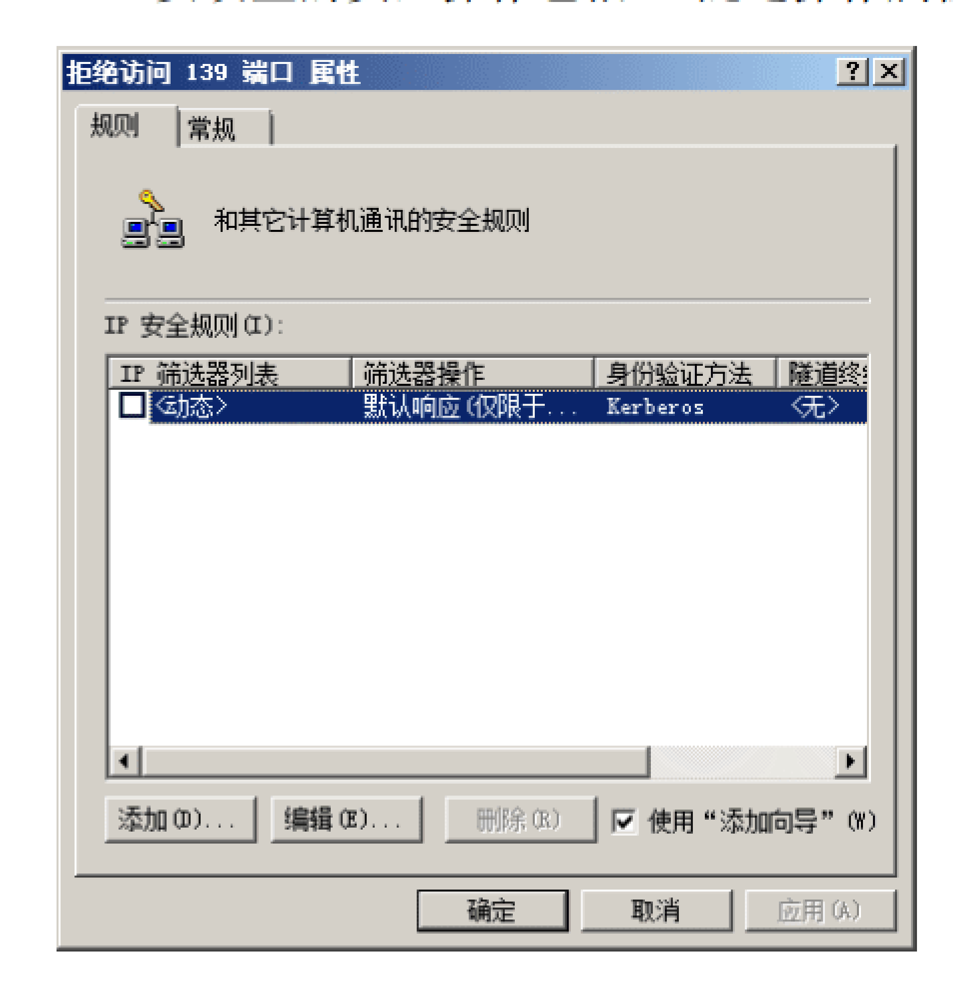


图 2-65　“拒绝访问 139 端口　属性”对话框

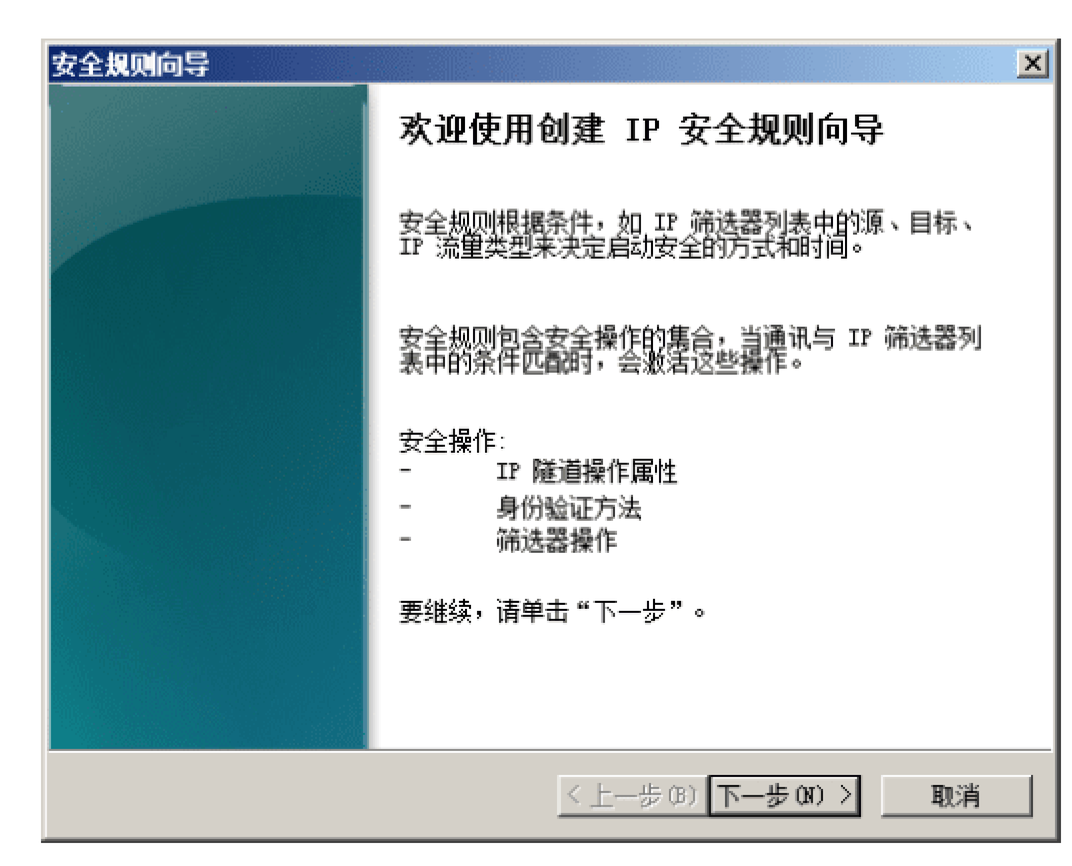


图 2-66　“安全规则向导”对话框

③ 单击“下一步”按钮，显示如图 2-67 所示的“隧道终结点”界面，选择“此规则不指定隧道”单选按钮，即可禁用该规则的隧道。如果想对特定隧道终结点使用隧道通信，则选择“隧道终结点由下列 IP 地址指定”单选按钮，并输入隧道终点的 IP 地址。

注意：因为无法为隧道通信镜像筛选器，所以必须配置两个规则，一个规则用于出站通信，另一个规则用于进站通信。对于出站通信规则，隧道终点是在隧道另一端的计算机的 IP 地址。对于进站通信规则，隧道终点是本地计算机上所配置的 IP 地址。

④ 单击“下一步”按钮，显示如图 2-68 所示的“网络类型”界面，选择“所有网络连接”单选按钮。可供选择的“网络类型”包括以下内容。

■ 所有网络连接：可以将此规则应用到在该计算机中创建的所有网络连接。
■ 局域网(LAN)：单选按钮，可以将此规则应用到在该计算机中创建的所有 LAN 连接。
■ 远程访问：可以将此规则应用到在该计算机中创建的所有远程或拨号连接。

⑤ 单击“下一步”按钮，显示如图 2-69 所示的“IP 筛选器列表”界面，选择新创建的“TCP139”筛选器。

⑥ 单击“下一步”按钮，显示如图 2-70 所示的“筛选器操作”界面，选择已经创建好的“拒绝访问 139 端口”筛选器即可。如果在此之前没有创建 IP 筛选器，也可以单击“添加”按钮立刻添加。

⑦ 单击“下一步”按钮，显示如图 2-71 所示的“正在完成安全规则向导”界面，取消选中“编辑属性”复选框。

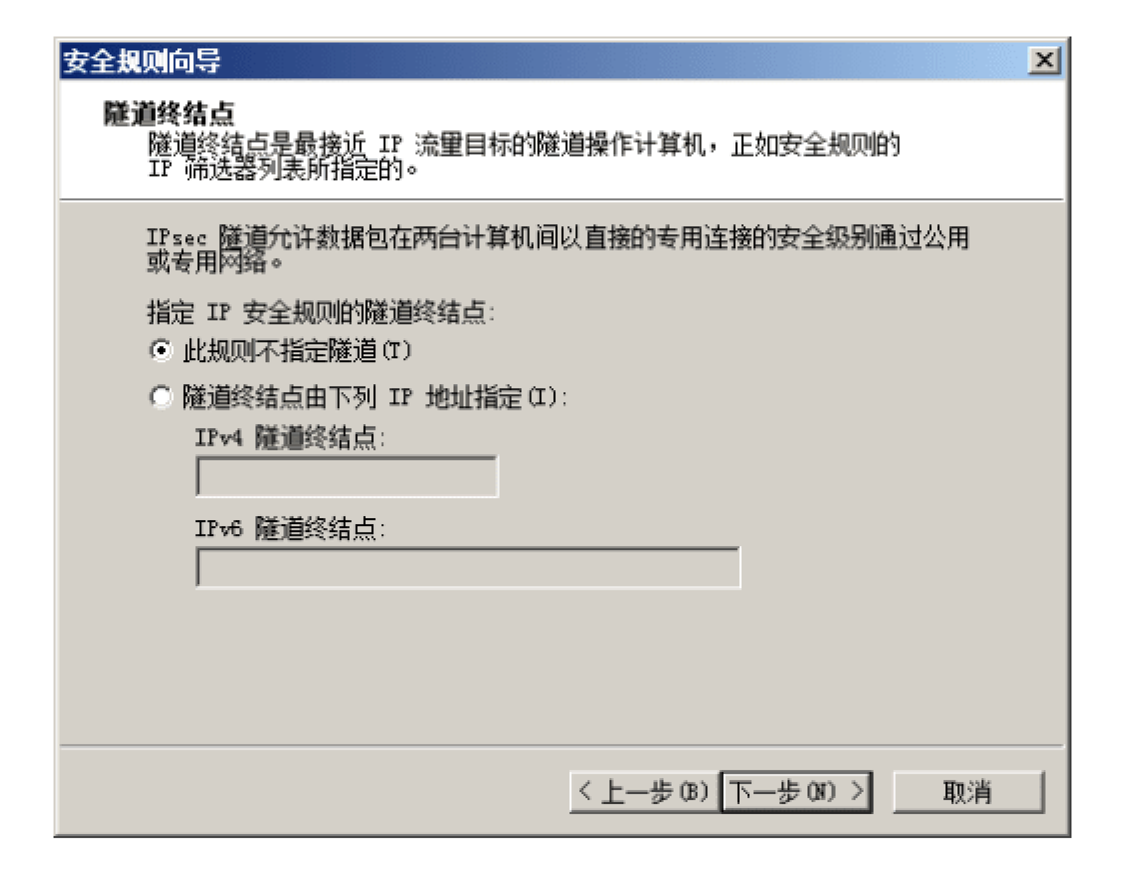


图 2-67 “隧道终结点”界面

图 2-68 “网络类型”界面

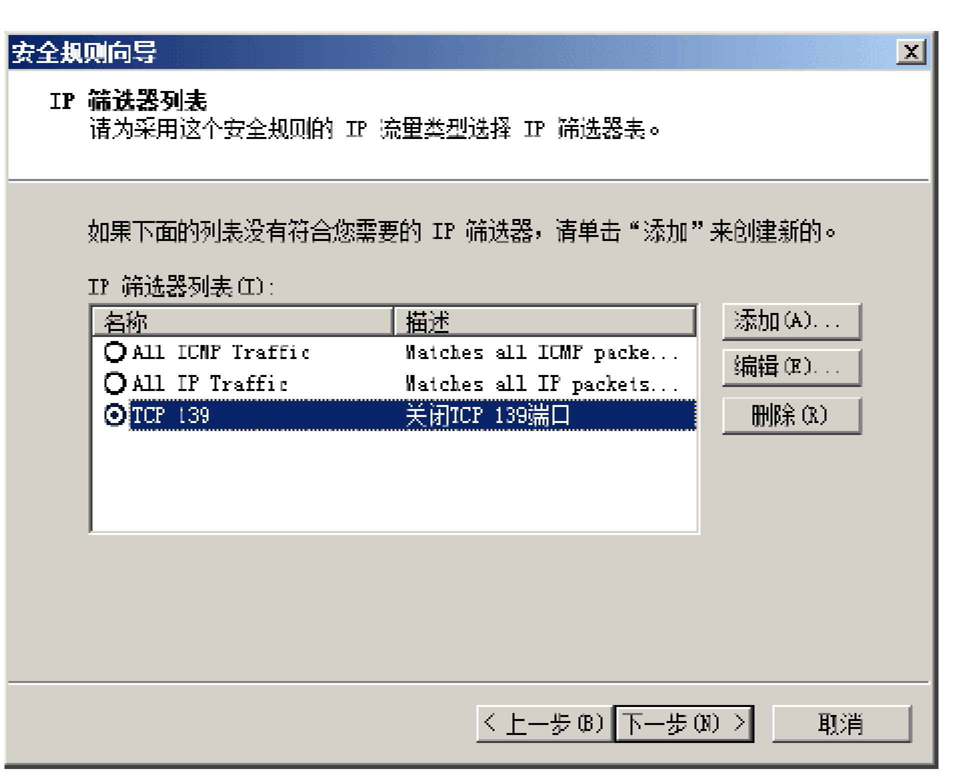


图 2-69 “IP 筛选器列表”界面



图 2-70 “筛选器操作”界面

⑧ 单击“完成”按钮，关闭“安全规则向导”对话框，返回“拒绝访问 139 端口 属性”对话框，如图 2-72 所示，新创建的安全规则已被添加到“IP 安全规则”列表中。

6. 分配 IP 安全策略

默认情况下，所有的 IP 安全策略都是未分配的，即不对任何网络访问进行保护和过滤。在“组策略管理编辑器”窗口的“IP 安全策略，在 Active Directory(coolpen.net)”中，右击想要分配的 IP 安全策略，并选择快捷菜单中的“分配”命令，如图 2-73 所示。稍后，该策略的“策略已指派”栏即可变为“是”状态，分配成功。



注意：当分配新的安全策略时，原有已分配策略将自动取消，变为“未分配”状态。

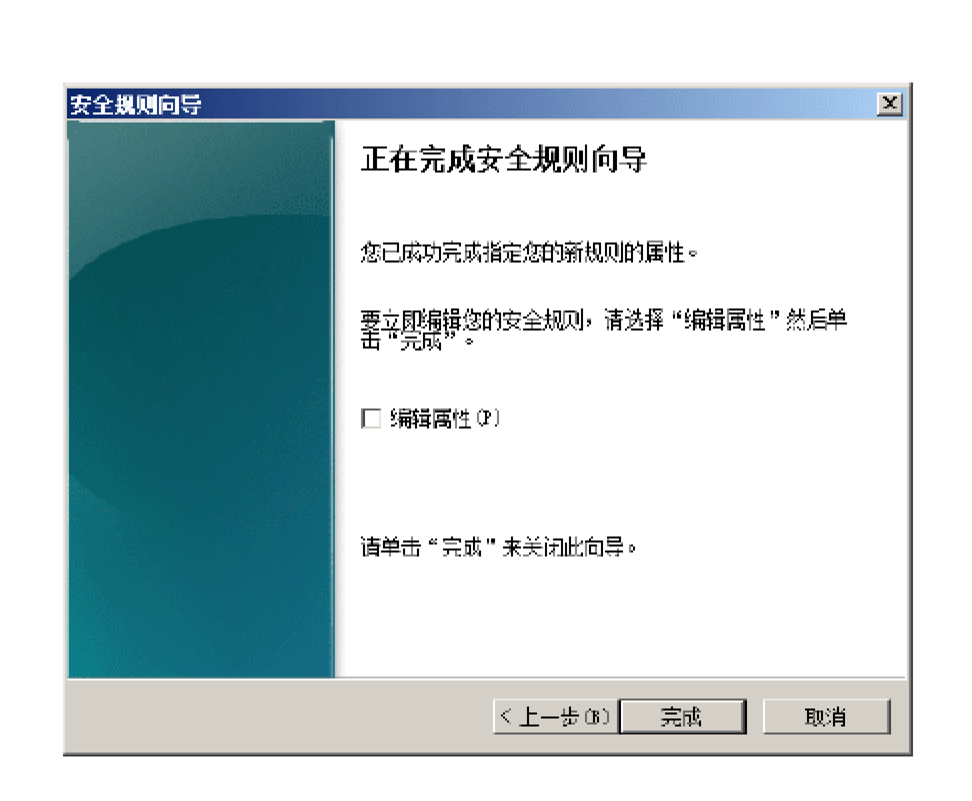


图 2-71　“正在完成安全规则向导”界面

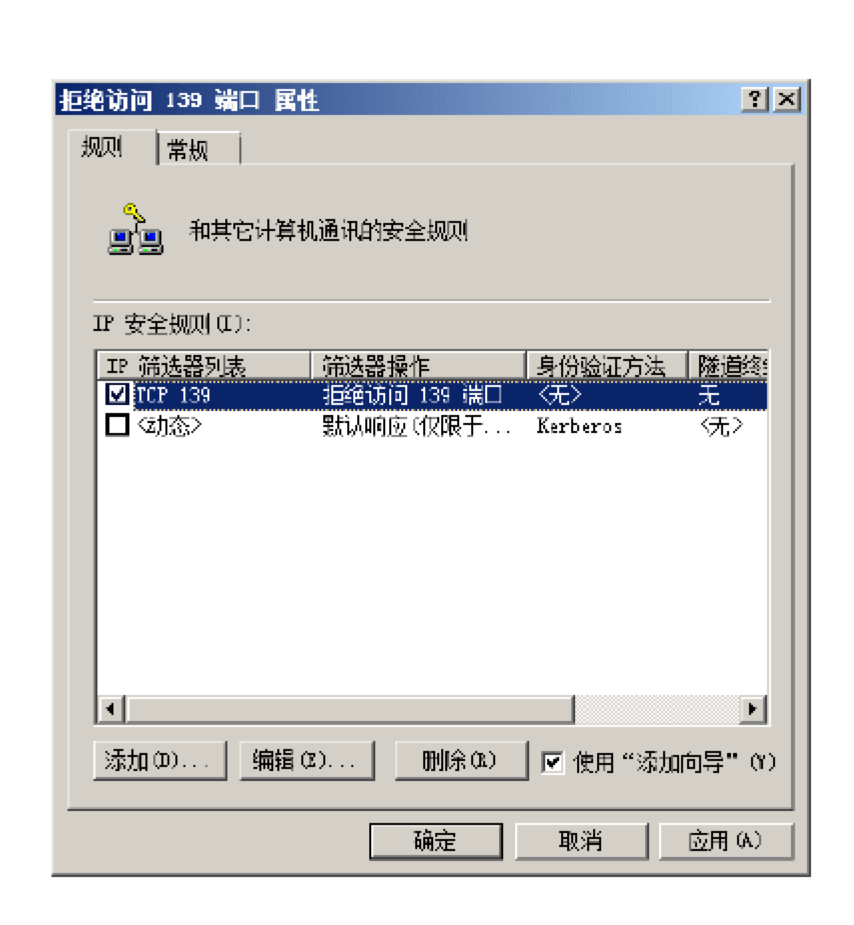


图 2-72　成功创建的 IP 安全规则

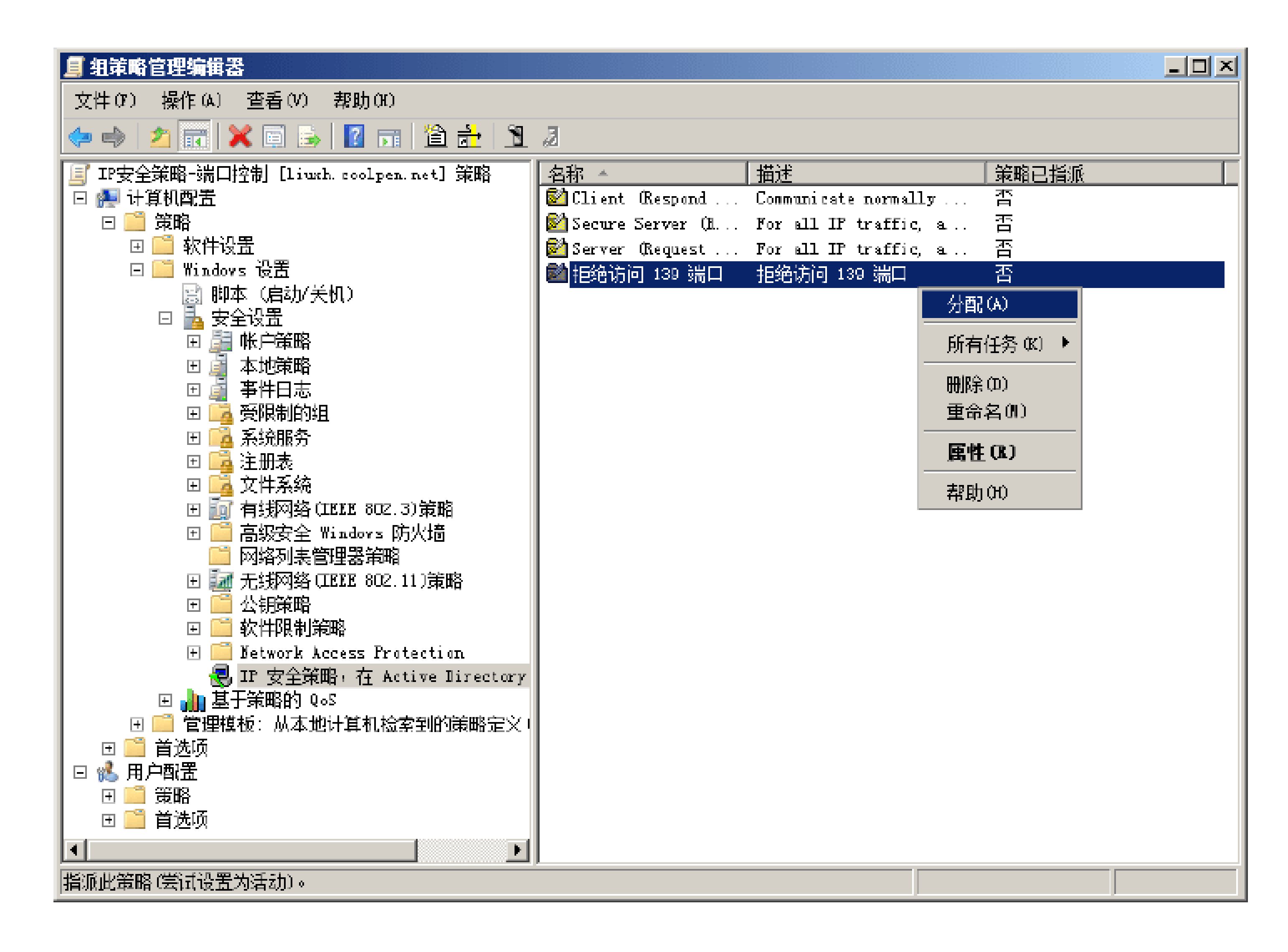


图 2-73　分配 IP 安全策略

2.7　系统漏洞安全

对于 Windows 操作系统而言，系统漏洞是无法避免的，新版操作系统弥补旧版本中漏洞的同时，还会引入一些新的漏洞。应对系统漏洞最有效的方法就是指定详细的修补策略，及时发现并弥补漏洞。漏洞除了系统（硬件、软件）本身固有的缺陷之外，还包括用户的不正当配置、管理、制度上的风险，或者其他非技术性因素造成的系统不安全性。

2.7.1　漏洞的特性

通常情况下，普通用户都是在产品供应商公布产品漏洞后，才得知漏洞消息的。从信息安全的角度看，

是先有漏洞和对漏洞的攻击的可能性，然后才会有补丁。漏洞是攻击者所要攻击的目标，而安装补丁是对漏洞的修补过程。漏洞是广泛存在的，不同的设备、操作系统、应用系统都会存在安全漏洞。

1. 漏洞的时间局限性

任何系统漏洞都是在用户的不断使用过程中被发现的，系统供应商随之采取新版本替代，或者发布补丁程序等方式弥补漏洞。但随着旧漏洞的消失，新环境下的新漏洞也将随时产生。因此，系统漏洞只是存在于特定时间和环境下的，即只能针对目标系统的系统版本、其上运行的软件版本，以及服务运行设置等实际环境。

2. 漏洞的广泛性

漏洞会影响到很大范围的软、硬件设备，包括操作系统本身及其支撑软件平台、网络客户端和服务器软件、网络路由器和安全防火墙等。换言之，在这些不同的软硬件设备中，都有可能存在不同的系统漏洞问题。例如，在不同种类的软、硬件设备之间，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞。

3. 漏洞的隐蔽性

安全漏洞是最常见的系统漏洞类型之一。入侵者借助于这些漏洞，可以绕过系统中的许多安全配置，从而实现入侵系统的目的。安全漏洞的出现，是因为在对安全协议的具体实现中发生了错误，是意外出现的非正常情况。而在实际的系统中，都会不同程度地存在各种潜在错误。因而所有系统中都存在安全漏洞，无论这些漏洞是否已被发现，也无论该系统的安全级别如何。在一定程度上，安全漏洞问题是独立于系统本身的理论安全级别而存在的。也就是说，并不是系统所属的安全级别越高，系统中所存在的漏洞就越少。

4. 漏洞的被发现性

漏洞是特定环境和时间内的必然产物，但必须发现后，才会被用来入侵系统或被弥补。在实际使用中，用户会发现系统中存在错误。入侵者会有意利用其中的某些错误，并使其成为威胁系统安全的工具，这时用户才会认识到这个错误是一个系统安全漏洞。系统供应商会尽快发布针对这个漏洞的补丁程序，纠正这个错误。这就是系统安全漏洞从被发现到被纠正的一般过程。

2.7.2 漏洞生命周期

漏洞所造成的安全问题具备一定的时效性，也就是说每一个漏洞都存在一个和产品类似的生命周期的概念。只有对漏洞生命周期的概念进行研究并且分析出一定的规律，才能达到真正解决漏洞危害的目的。

漏洞生命周期的定义：漏洞从客观存在到被发现、利用，到大规模危害和逐渐消失，这期间存在一个生命周期，该周期被称为漏洞生命周期。

以“冲击波(MSBlaster)”蠕虫病毒为例，漏洞生命周期包括如下 5 个基本阶段。

(1) 发现漏洞

2003 年 7 月 16 日，微软公司公布了 MS03-026 Microsoft Windows DCOM RPC 接口远程缓冲区溢出漏洞，该漏洞影响 Windows 2000、Windows XP、Windows Server 2003 系统。

(2) 弥补漏洞

2003 年 7 月 16 日，微软公司公布了 MS03-026 补丁用于修补该漏洞。然而，在微软公布该漏洞后，

网络上仍有零星的恶意攻击者利用该漏洞进行入侵。

(3)　利用漏洞的病毒大肆爆发

2003 年 8 月 11 日，爆发了利用上述 Windows 漏洞的“冲击波”蠕虫病毒。

(4)　病毒出现变种

2003 年 8 月 18 日，出现了一个利用同样原理进行蔓延的“冲击波清除者”病毒，该蠕虫专门清除原来的冲击波病毒，然而这个病毒却消耗了大量的 Internet 带宽，导致互联网连续 3 个月的性能显著下降。

从蠕虫病毒爆发后全球 Windows 用户开始安装 MS03-026 补丁修补该漏洞，网络运营商开始设法阻止蠕虫蔓延，计算机防病毒厂商加入蠕虫特征进行查杀。

(5)　逐渐消失

2004 年 1 月，蠕虫传播开始明显被遏制，微软公司估计全球有 1000 万台主机受到感染。从整个事件开始到结束所对应的 5 个阶段如表 2-3 所示。

表 2-3　漏洞的生命周期

阶　段	事　件	描　述
第 1 阶段	系统漏洞被发现，并发布安全公告	由于软件设计者初期考虑不周等因素导致漏洞客观存在，漏洞研究人员发现漏洞并报告相关厂商，厂商向用户发布安全公告，并提供升级补丁程序
第 2 阶段	借助于漏洞进行传播的病毒开始出现，并传播	攻击者对安全补丁进行逆向工程，编写利用漏洞的攻击程序并发布。但是用户在漏洞管理方面的疏忽，如没有在第一时间安装升级补丁程序，就会为蠕虫爆发创造条件。此阶段漏洞的危害较小
第 3 阶段	利用漏洞的蠕虫病毒大肆爆发	蠕虫在互联网或者局域网上利用系统漏洞大规模传播，导致网络堵塞或者瘫痪
第 4 阶段	系统漏洞被修复，但仍有发作	由于安装系统补丁，蠕虫丧失感染目标，已经感染的主机逐步清除使蠕虫源减少。少数没有安装补丁的主机数量减少，对网络的影响不大
第 5 阶段	漏洞影响逐渐消失	一段时间过后，由于系统升级或者完成系统补丁安装工作，或者使用新的软件版本，漏洞造成的影响逐步消失

2.7.3　漏洞管理流程

网络防火墙的访问控制和入侵检测功能，并不能对系统存在的漏洞进行有效防御和阻止；杀毒软件更是如此，只有当借助于漏洞入侵的病毒发生作用时，才会有所反映，因此这些防御方法只能作为网络管理员的一种辅助手段。要从根本上解决利用漏洞进行攻击的问题，就需要对漏洞产生的原因、漏洞的生命周期进行研究，同时配合人为的管理模式，建立行之有效的管理机制，并通过漏洞管理类的产品辅助执行漏洞管理。

1. 安全策略

安全策略是指确保服务器、网络设备、客户端计算机、网络安全设备能够正常工作的安全配置。大多数网络设备都可以提供丰富的安全功能，并且部分功能已经默认启用，管理员也可以根据实际需要，制定更加详细的安全策略。

2. 漏洞预警

漏洞预警工作通常由产品供应商完成，即确保在发现漏洞后，第一时间告知用户，如果没有相应的补丁程序，还应给出临时的解决方案等。这就要求漏洞管理产品的厂商应该有基础的漏洞研究、跟踪以及提供临时解决方案的能力。

3. 漏洞检测

执行检测工作之前需要对网络的资产进行发现和跟踪，以便快速、准确的确定产生漏洞的计算机或网络设备。作为网络管理员，必须周期性地对网络中地网络资产进行检测，要求漏洞管理工具在保证一定效率的前提下，具有较高的准确性。需要注意的是，并不是检测到的漏洞越多越好，而是要对检测的有效性进行验证和分析。

4. 漏洞统计分析

在漏洞检测完成之后，需要通过具体的报告和数据来对资产的风险进行评估、分析，清楚地显示漏洞分布状况、详细描述以及相应的解决方案。需要注意的是，要对网络中的资产风险进行分类，以便于对后续的漏洞修补工作进行优先级区分。这一过程也可以通过购买专业的漏洞管理设备或者安全服务来完成。

5. 漏洞修补

通过统计分析的结果指定切实可行的漏洞修补方案，并以合理的方式通知用户，例如：可以通过自动更新服务器来提供最新的漏洞修补程序；用户可以按需下载，也可以由服务器自动分发完成。需要注意的是，要注意补丁来源的合法性，以及补丁的安全性。通常情况下，必须对补丁程序进行小范围内的安全性测试、兼容性测试，确定补丁不会影响到业务系统的正常运行后，才可以大范围分发。

6. 漏洞审计、跟踪

必须在网络中部署完善的漏洞审计机制，即对于新接入或启用的计算机或网络设备，进行补丁状态检测，如果不能满足安全要求，则拒绝继续访问，或通过其他措施使其可以获得所需的安全补丁。这个过程可以通过操作系统厂商、第三方的补丁管理软件或者专业的安全服务完成。

7. 其他问题

一个完善的漏洞管理机制能够有效地保证人为的管理疏漏不被攻击者利用，对于大多数利用漏洞的攻击会十分有效。网络管理人员在制定漏洞管理流程的时候要根据实际情况进行细化或者裁减，确保漏洞管理的高效、灵活、实用。漏洞管理流程应该注意的其他问题包括：

- 工作流程标准化。
- 尽量使用专业的、自动化的漏洞管理工具，尽量避免人为操作。
- 尽量不要中断企业的业务流程，保证业务的正常运行。
- 漏洞修补尽量安排在晚上或者业务不繁忙的时候运行。
- 在测试环境中模拟测试通过，在确保不影响当前业务的状态下，实施漏洞修补工作流程。
- 针对不同的操作系统要准备不同的版本。

2.7.4 漏洞修补方略

大多数蠕虫病毒都是通过系统漏洞进行传播的，同时网络扫描和利用系统漏洞，也是“黑客”最常用

的攻击手段之一。因此，做好网络的安全保障，必须做好漏洞补丁的安装管理工作。对于个人用户而言，系统漏洞修补主要是安装官方网站发布的补丁，而在服务器或者网络中大规模部署补丁通常是一项非常重要的工作。安装之前，必须先在实验环境中进行测试和分析，然后才可以在网络中大规模部署。

1. 环境分析

知己知彼，百战不殆。只有真正了解网络内部状况，才能有效地实施漏洞修补。例如，及时掌握网络资产情况、设备运行状态，包括网络中运行的设备型号、厂商、操作系统种类、版本等。同时还要了解企业的主要业务系统及重要的数据，根据需要划分安全等级，以确定安装补丁的紧急程度和修补时间。

2. 补丁分析

用户计算机系统信息、硬件等变化，都可能导致无法正确安装官方发布的系统漏洞补丁，甚至安装后还会导致一系列的问题。因此，部署之前一定要针对用户系统环境进行测试，切不可盲目地安装补丁，否则将带来许多意想不到的问题，其中包括：

- 导致系统兼容性出现问题，甚至不能使用。
- 系统崩溃，无法正常工作。
- 部分功能无法使用。

在得到补丁以后，正确的做法应该是：

- 在测试环境中，测试对业务系统的影响，以及兼容性。
- 了解补丁自身的稳定性。
- 查看补丁是否还存在漏洞。
- 在大规模部署之前，进行小范围的短时间的联机测试。

在测试的过程中，应做好详细的测试记录，了解补丁程序和与其相关的组件对象之间的兼容性，对原有系统功能的影响，是否可以卸载，是否可以“回滚”等。

3. 分发安装

对于网络用户而言，管理员可以通过组策略、SMS、WSUS 等多种方法，将已获得的系统补丁分发到客户端。其中，WSUS 为微软公司提供的专用于补丁更新的服务组件，可以根据客户端实际情况，自动将补丁程序分发到用户或计算机，建议使用这种方法。

2.7.5 漏洞扫描概述

在网络安全体系的建设中，单机安全扫描是一种花费低、效果好、见效快、与网络运行相对独立、安装运行简单的工具，可以大规模减少网络管理员的手工劳动，有利于保持全网安全的统一和稳定。

目前，市场上有很多漏洞扫描工具，按照不同的技术(基于网络的、基于主机的、基于代理的、Client/Server)、不同的特征、不同的报告方法，以及不同的监听模式，可以分成很多种。不同的产品之间，漏洞检测的准确性差别较大，这就决定了生成报告的有效性上也有很大区别。选择正确的漏洞扫描工具，对于提高系统的安全性非常重要。

1. 漏洞扫描的必要性

一般情况下，在网络边界处都会部署硬件或软件防火墙。防火墙作为不同网络或网络安全域之间信息

的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。虽然防火墙是提供信息安全服务、实现网络和信息安全的基础设施，但是，它也存在着一定的局限性。

“外紧内松”是一般局域网络的特点，一道严密防守的防火墙其内部的网络也有可能是防范松懈的。

2. 扫描工具的技术性能

采用漏洞扫描工具是保护系统安全的重要一步。当决定使用漏洞扫描以后，接下来的是如何选择满足企业需要的合适漏洞扫描软件或者工具。

选择扫描工具时，应当注意以下几个方面的问题。

- 漏洞库中的漏洞数量。
- 扫描工具的易用性。
- 是否可以生成漏洞报告，包括内容是否全面、是否可配置、是否可定制、报告的格式和输出方式等。
- 对于漏洞修复行为的分析和建议。是否只报告存在哪些问题、是否会告诉应该如何修补这些漏洞。
- 安全性。由于有些扫描工具不仅仅只是发现漏洞，而且还进一步自动利用这些漏洞，扫描工具自身是否会带来安全风险。
- 工具性能及价格。

2.7.6 漏洞扫描工具——MBSA

MBSA 全称 Microsoft Baseline Security Analyzer，此工具允许用户扫描一台或多台基于 Windows 系统的计算机，以及发现常见安全方面的配置错误，并检查操作系统和已安装的其他组件，及时通过推荐的安全更新进行修补。MBSA 支持的系统平台包括 Windows NT/2000/XP/2003/2008，支持类型涵盖了微软公司的大部分产品。

1. 扫描模式

MBSA 允许扫描一台或者多台计算机：

- 单台计算机。MBSA 最简单的运行模式是扫描单台计算机。默认情况下，将扫描本地计算机，管理员也可以通过指定计算机名或 IP 地址方式，使其扫描其他计算机。扫描远程计算机时，当前用户账户必须拥有目标计算机的远程访问权限。
- 多台计算机。如果选择“选取多台计算机进行扫描”时，可以选择通过输入域名扫描整个域，或指定一个 IP 地址范围并扫描该范围内的所有基于 Windows 的计算机。



注意：扫描远程单台主机或其他网段的计算机时，必须使用具有相关权限的用户账户。在进行“自动扫描”时，用来运行 MBSA 的账户也必须是管理员或者是本地管理员组的成员。

2. 扫描类型

MBSA 支持两种类型的扫描模式：

- MBSA 典型扫描。MBSA 典型扫描将执行扫描并且将结果保存在单独的 XML 文件中，这样就可以在 MBSA 查看器中进行查看。可以通过 MBSA GUI 方式(mbsa.exe)或 MBSA 命令行方式(mbsacli.exe)

进行 MBSA 典型扫描，扫描内容包括所有可用的 Windows、IIS、SQL 和安全更新检查。每次执行 MBSA 典型扫描时，都会为每一台接受扫描的计算机生成一个安全报告，并保存到正在运行 MBSA 的计算机中。

- HFNetChk 典型扫描。HFNetChk 典型扫描将只检查缺少的安全更新，并以文本的形式将扫描结果显示在命令行窗口中。与以前独立版本的 HFNetChk 处理方法完全相同。这种类型的扫描可以通过带有“/xmlout”开关参数(指示 MBSA 工具引擎进行 HFNetChk 扫描)的 mbsacli.exe 来执行。

3. 查看安全报表

每次执行 MBSA 典型扫描时，都会为每一台接受扫描的计算机生成一个安全报表，并保存在正在运行 MBSA 的主机上。

安全报表默认的文件格式为 XML。可以按照计算机名、扫描日期、IP 地址或安全评估对这些报告进行排序。

4. 网络扫描

MBSA 最多可以允许从服务器同时对 10000 台计算机进行远程漏洞扫描。在防火墙或路由器将两个网络分开的多域环境中(两个单独的 Active Directory 域)，TCP 的 139 端口和 445 端口以及 UDP 的 137 端口和 138 端口必须开放，以便 MBSA 连接和验证所要扫描的远程网络主机。

5. 操作系统检查

MBSA 对被扫描计算机中的 Windows 操作系统进行扫描，并检测是否存在以下漏洞。

(1) 管理员组成员权限

该项检查将确定并列出属于本地管理员组的用户账户。如果检测出的单个管理员账户数量超过两个，则该工具将列出这些账户名，并将该检查标记为一个潜在的安全漏洞。一般情况下，建议将管理员的数量保持在最低限度，因为管理员对计算机具有完全控制权。

(2) 审核

该项检查将确定在被扫描的计算机上是否启用了系统审核功能。Windows 系统的审核特性可跟踪和记录系统上的特定事件，如成功的和失败的登录尝试。通过监视系统的事件日志，可以发现潜在的安全问题和恶意活动。

(3) 自动登录

该项检查将确定在被扫描的计算机上是否启用了“自动登录”功能，以及登录密码是否在注册表中以明文方式存储。如果“自动登录”已启用并且登录密码以明文形式存储，则安全报表就会将这种情况作为一个严重的安全漏洞反映出来。如果“自动登录”已启用而且密码以加密形式存储在注册表中，那么安全报表就会将这种情况作为一个潜在的安全漏洞标记出来。默认情况下，Windows Server 2008 禁止“自动登录”。



注意：如果扫描结果中提示“Error Reading Registry”(读取注册表时出错)消息，则表示远程注册表服务可能还未启用。

(4) 自动更新

该项检查将确定是否在被扫描的计算机上启用了自动更新功能，以及详细的配置情况。通常情况下，

用户可以通过多种方式获取和安装更新，例如直接访问 Windows Update 站点、组策略远程部署、架设 WSUS 服务器等。当用户使用直接下载更新方式之外的其他方式时，扫描结果中可能会出现相关的安全警告信息，提示自动更新没有正确配置，此时不必理会。

(5) 域控制器

该项检查将确定正在接受扫描的计算机是否为域控制器，这主要是针对 Windows Server 2003 和 Windows Server 2008 系统而言的。在 Windows 域网络中，域控制器的地位和作用是非常重要的，不仅掌管着所有网络资源的安全访问，而且存储着所有网络用户的身份验证信息，如果存在安全漏洞，则后果不堪设想。基于上述原因，域控制器应该被视为需要加强保护的关键资源。应确认当前网络是否需要将这台计算机作为域控制器，并确认是否采取了相应的步骤来加强这台计算机的访问安全。

(6) 文件系统

该项检查将确定在每个分区使用的文件系统类型。NTFS 具有访问控制功能，是一个安全的文件系统，因此，服务器所有分区均使用该文件系统，如果使用 FAT32 文件系统，则扫描结果中将报警。


注意：为了使该检查成功执行，驱动器必须通过管理驱动器共享来实现共享。

(7) 来宾账户

该项检查将确定在被扫描的计算机上是否启用了系统内置的来宾账户。来宾账户主要视为临时用户提供的，默认情况下是禁用的。当一名用户在计算机或域上没有账户，或者在计算机所在的域信任的任何一个域中没有账户时，可使用这种账户登录到运行 Windows NT/2000/XP/2003/Vista/2008 系统的计算机。在使用简单共享的 Windows XP/Vista 计算机上，作为安全模型的一部分，网络上的所有用户连接都将映射到来宾账户。

如果在 Windows NT/2000/XP/2003/Vista/2008 计算机上已启用来宾账户，则此时将在安全报表中作为一个安全漏洞标记出来。如果在使用简单文件共享的 Windows XP/Vista 计算机上已启用来宾账户，则这种情况将不会作为安全漏洞标记出来。

(8) Windows 防火墙

该项检查将确定是否在被扫描的计算机上对所有的活动网络连接启用 Windows 防火墙，这主要是针对 Windows XP/2003/2008 系统而言的。如果已经启用防火墙，则还将对其开放的入站端口进行检测。如果上述系统的 Windows 防火墙没有开启，或者开放了存在安全漏洞的端口，则扫描结果中将出现警告信息。

(9) 本地账户密码

该项检查将找出使用空白密码或简单密码的所有本地用户账户。Windows 2000/XP/2003 系统的管理员账户密码均可以设置为空，因此存在很大的安全隐患。在 Windows Server 2008 系统中，必须设置符合相应复杂程度的安全密码，才允许启用管理员账户。因此该项扫描只适用于 Windows 2000/XP/2003 系统，如果本地用户账户密码符合下列条件之一，就会出现警告：

- 密码为空白。
- 密码与用户账户名相同。
- 密码与计算机名相同。
- 密码使用“password”一词。
- 密码使用“admin”或“administrator”一词。



提示：该项检查可能会花较长时间，这取决于计算机上的用户账户数量。因此，管理员可能需要在扫描它们所在网络的域控制器前禁用该检查。

(10) 密码过期

该项检查将确定是否有本地用户账户设置了永不过期的密码。密码应该定期更改，以降低遭到密码攻击的可能性。

(11) 限制匿名用户

该项检查将确定被扫描的计算机上是否使用了 RestrictAnonymous 注册表项来限制匿名连接。允许匿名连接本身就是一个很危险的系统漏洞，何况匿名用户还可以列出某些类型的系统信息，其中包括用户名及其详细信息、账户策略和共享名，因此必须对安全要求严格的服务器限制此项功能，以使匿名用户无法访问。

(12) 共享资源

该检查将确定在被扫描的计算机上是否存在共享文件夹。扫描报告将列出在计算机上发现的所有共享内容，其中包括管理共享及其共享级别和 NTFS 级别的权限。通常情况下，应关闭系统中非必要的共享目录，尤其是服务器更应如此。扫描结果中将列出所有的系统默认共享，和用户后期设置的重要资源共享。

(13) 检查是否存在不必要的服务

该检查将确定被扫描计算机上的 services.txt 文件中是否包含已启用的服务。services.txt 文件是一个可配置的服务列表，这些服务都不应该在被扫描的计算机上运行。此文件由 MBSA 安装并存储在该工具的安装文件夹中。该工具的用户应配置 services.txt 文件，以便包括在各台被扫描的计算机上所要检查的那些特定服务。默认情况下，与该工具一起安装的 services.txt 文件包含下列服务：

- MSFTPSVC(FTP)。
- TlntSvr(Telnet)。
- W3SVC(WWW)。
- SMTPSVC(SMTP)。

服务是一种程序，只要计算机在运行操作系统，它就在后台运行。服务不要求用户必须进行登录。服务用于执行不依赖于用户的任务，如等待信息传入的传真服务。

6. 安全更新检查

MBSA 对在被扫描的计算机中的安全更新列表进行扫描，并检测是否存在由于安装更新补丁产生的新漏洞。该项检查将确保具有针对下列产品和组件的最新服务包和安全更新：

- Windows NT 4.0(除非通过 mbsacli.exe /xmlout 进行扫描，否则只能进行远程扫描)。
- Windows 2000。
- Windows XP。
- Windows Server 2003。
- Windows Vista。
- Windows Server 2008。
- Internet Explorer 5.01 和后续版本。
- Windows Media Player 6.4 和后续版本。

- IIS 4.0 和后续版本。
- SQL Server 7.0/2000/2005(包括 Microsoft Data Engine)。
- Exchange Server 5.5/2000/2003/2007(包括 Exchange Admin Tools)。
- Microsoft Office(只能进行本地扫描)。
- Microsoft Data Access Components(MDAC)2.5/2.6/2.7/2.8。
- Microsoft Virtual Machine。
- MSXML 2.5/2.6/3.0/4.0/5.0/6.0。
- BizTalk Server 2000/2002/2004/2006。
- Commerce Server 2000/2002。
- Microsoft Content Management Server(MCMS)2001/2002。
- SNA Server 4.0、Host Integration Server(HIS)2000 和 2004。

7. 桌面应用程序检查

MBSA 对在被扫描计算机中的桌面应用程序进行扫描，并检测是否存在以下漏洞。

(1) IE 安全区域

该项检查将列出被扫描计算机上所有本地用户当前采用的 IE 区域安全设置，并给出合理建议。

IE 内容区域将 Internet 或 Intranet 分成了具有不同安全级别的区域。对于每个安全区域，可以选择相应的安全级别，或者自定义安全设置。Microsoft 建议，对于不能确定是否可信任的区域内的站点，应将安全性设置为高。自定义选项为高级用户和管理员提供了针对所有安全选项的更多的控制权，其中包括下列几项：

- 对文件、ActiveX 控件和脚本的访问。
- 提供给 Java 小程序的功能级别。
- 带有安全套接字层(SSL)身份验证的站点身份指定。
- 带有 NTLM 身份验证的密码保护(根据服务器所在的区域，Internet Explorer 可以自动发送密码信息，提示用户输入用户名和密码信息，或者干脆拒绝任何登录请求)。

(2) 面向管理员的 IE 增强安全配置

该检查可识别出运行 Windows Server 2008 系统的计算机上是否已经启用针对管理员的 IE 增强安全配置(Enhanced Security Configuration)。如果已经安装了针对管理员的 IE 增强安全配置，这一检查还会识别出禁用该 IE 增强安全配置的管理员。

(3) 面向非管理员的 IE 增强安全配置

该检查识别出在运行 Windows Server 2008 系统的计算机上，是否已经启用用于非管理员的用户的 Internet Explorer 增强安全配置(Enhanced Security Configuration)。如果已经安装了针对非管理员的 Internet Explorer 增强安全配置，这一检查还会识别出禁用该 Internet Explorer 增强安全配置的非管理员用户。

(4) Office 安全配置和分析宏保护

该检查将对每个用户逐一确定 Microsoft Office 2003、Office 2000 和 Office 97 宏保护的安全级别。MBSA 还将对 PowerPoint、Word、Excel 和 Outlook 进行检查。

宏能够将重复的任务自动化。这样可以节省时间，但也会被用于传播病毒，例如，当用户打开包含恶意宏的受感染文档时，就会使恶意宏蔓延到系统上的其他文档，或者传播给其他用户。

第 3 章　活动目录安全

Windows Server 2008 活动目录域名服务(ADDS)在安全方面有了很大的改进，同时使部署和管理 ADDS 变得更加轻松。其中，只读域控制器(RODC)是一项非常重要的技术。这是因为许多用户是具有许多分公司的全球性组织，多数为销售公司或生产网点，带宽有限，域控制器的安全性很差。此时，要做到既满足用户快速登录的需求，又能确保域控制器的安全，就要用到 RODC。

关键词

- 活动目录安全管理
- 活动目录数据库

3.1 活动目录安全管理

Active Directory 是一个分布式的数据库，包含的对象信息通常分布在多台不同的计算机上，用于提供安全认证和网络资源管理。安装 Active Directory 服务的计算机被称为域控制器，在 Active Directory 架构中，域控制器可以担当多种角色，例如，全局编录服务器、操作主机以及单一域控制器等。在大、中型 Windows 域网络中，必须详细指派每台域控制器的角色，以免产生网络管理上的混乱，导致不必要的安全问题。

3.1.1 全局编录

全局编录(Global Catalog，GC)是域林中所有对象的集合，是一台特殊的域控制器，主要存储林中主持域的目录中所有对象的完全副本，以及所有其他域中所有对象的部分只读副本。默认情况下，在活动目录中创建的第一个域控制器为全局编录服务器，其他域控制器也可以被指派为全局编录服务器，用于实现网络负载平衡和冗余。全局编录服务器负责响应网络中所有的全局编录查询，一旦出现问题，用户将无法查询和登录。建议网络安全要求较高的用户配置多台全局编录服务器，以提高系统的可用性和可靠性。但需要注意的是，网络中 GC 之间的复制可能会增加一定的网络带宽开销。


注意：当林中只有一个域时，则不必在登录时从全局编录获取通用组成员身份。因为 Active Directory 可以检测到林中没有其他域，并将阻止向全局编录查询此信息。

1. 概述

GC 服务器中存储的数据都是用户搜索操作中最常用的部分，可以为用户提供高效的搜索，避免再去调用域控制器中的 Active Directory 数据库对网络性能带来的影响。全局编录的主要功能如下。

(1) 查找对象

全局编录允许用户在林中的所有域中搜索目录信息，无论目标数据存储在什么位置，都将以最快的速度和最低的网络流量在林中执行搜索。

(2) 提供用户主体名称身份验证

当验证域控制器无法识别用户账户时，全局编录服务器会解析主体名称(User Principal Name，UPN)，从而确定其属于林中的哪个域。例如，如果某账户属于 hs.coolpen.net，并且使用 liuxh@hs.coolpen.net 的 UPN 名称从一台位于 heb.coolpen.net 的计算机上登录，则此时 heb.coolpen.net 无法为该用户提供身份验证，必须与全局编录服务器联系，经确认后该用户账户方可顺利登录。

(3) 验证林内的对象引用

域控制器使用全局编录验证对林内其他域的对象的引用。当域控制器保留其属性包含对其他域中对象引用的目录对象时，域控制器将通过与全局编录服务器联系来验证引用的合法性。

(4) 提供多域环境中的通用组成员身份信息

域控制器可以始终发现其域中任何用户的本地组和全局组成员身份，并且这些组的成员身份信息是不被存储在全局编录服务器上的。在单域林环境中，域控制器可以始终发现通用组成员身份，但通用组可以

包含来自不同域的成员，因此将通用组的成员身份信息复制到全局编录服务器，可以提供更广范围的账户身份信息验证。在多域林环境中的用户登录到允许通用组的域时，域控制器必须与全局编录服务器联系，以检索用户可能在其他域中具有的任何通用组成员身份。



提示：如果用户登录到通用组可用的域时，全局编录服务器不可用，则用户的客户端计算机可以使用缓存凭据登录；如果用户在此之前并未登录到过该域，则用户只能登录到本地计算机。

2. 添加全局编录服务器

默认情况下，每个域林中只有一台全局编录服务器，即根域控制器。但为了提升网络安全性，往往需要添加一台或者多台全局编录服务器，实现冗余和负载均衡。在根域控制器上进行如下操作，即可将其子域控制器或备份域控制器提升为全局编录服务器。

① 依次选择“开始”→“管理工具”→“Active Directory 站点和服务”，打开“Active Directory 站点和服务”窗口，依次展开 Sites→Default-First-Site-Name(系统默认站点名称)→Servers→TIANJL(子域控制器)→NTDS Settings，如图 3-1 所示。

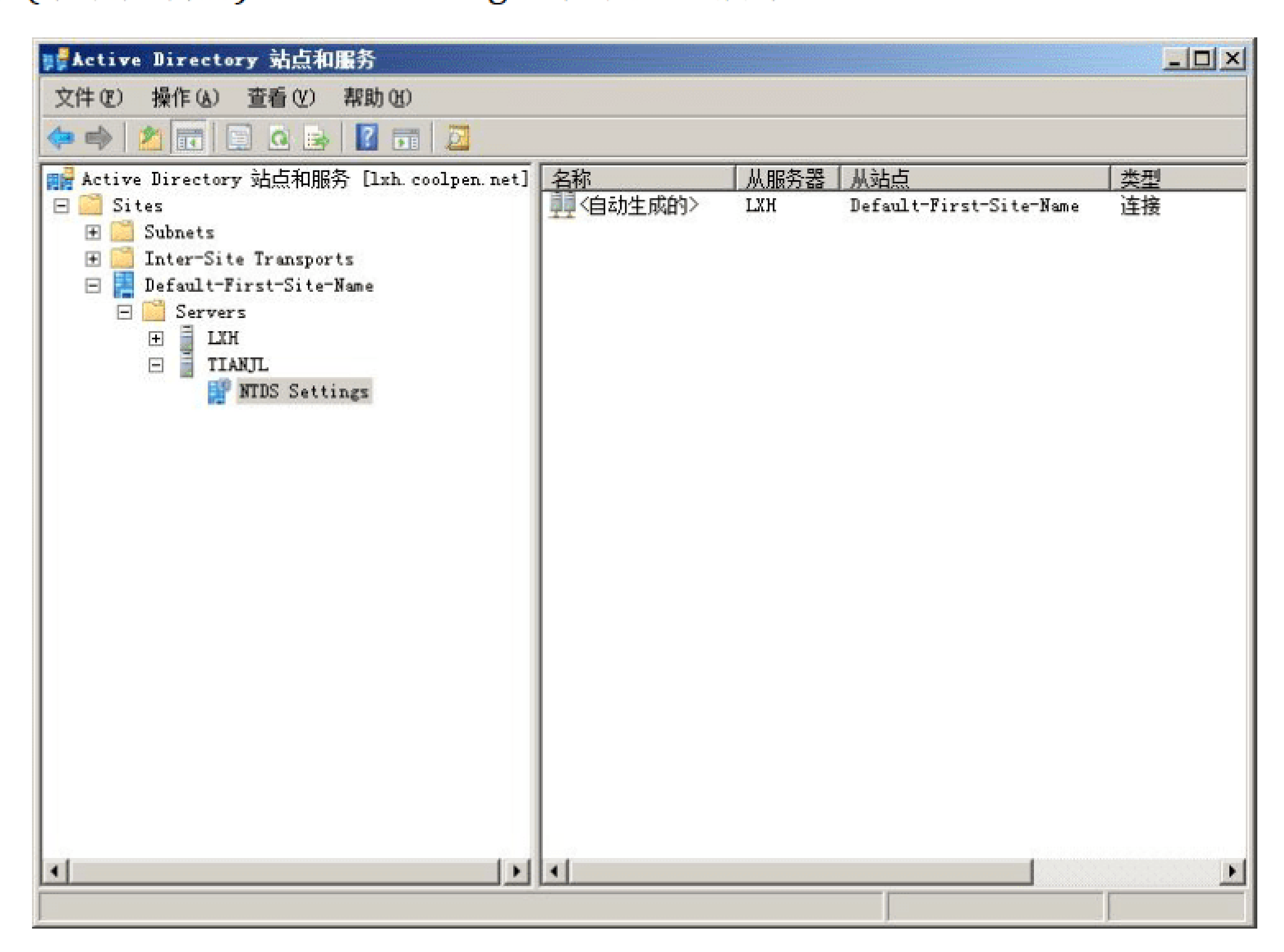


图 3-1　“Active Directory 站点和服务”窗口

② 右击 NTDS Settings 并选择快捷菜单中的“属性”命令，显示如图 3-2 所示的“NTDS Settings 属性”对话框，选中“全局编录”复选框。

③ 单击“确定”按钮，显示如图 3-3 所示的“Active Directory 域服务”对话框。提示所选子域是当前域中的结构主机角色，不适宜用作全局编录服务器。

④ 单击“是”按钮确认，并单击“确定”按钮保存设置，即可将该子域提升为全局编录服务器。

如果在一台已经是全局编录服务器的控制器上，取消其“全局编录”身份之后，系统将立即停止对全局编录服务器服务端口(默认使用 3268 和 3269 端口)的监听。同时，开始执行数据库清理工作，清理的时间比较长，大约每个小时从域控制器删除 2000 个对象，直到清理完成为止。Windows Server 2008 的 Active Directory 服务允许管理员删除全局编录服务器，但是不允许将全部全局编录服务器删除，否则用户账户将

无法正常登录，Active Directory 将不能正常运行。



图 3-2 “NTDS Settings 属性”对话框

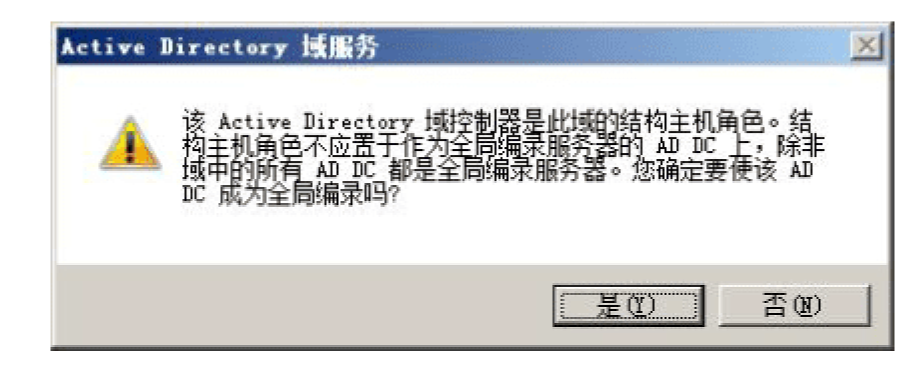


图 3-3 “Active Directory 域服务”对话框



注意：设置完成，并不代表全局编录服务器已经提升完成，全局编录数据库同步需要时间。

3.1.2 操作主机

默认情况下，Active Directory 域中的第一台域控制器承载着整个林的所有操作主机(Operations Masters，OM)角色，也称为灵活单主机操作(Flexible Single Master Operation，FSMO)。操作主机是 Active Directory 数据库中的特殊对象，具备此类角色的域控制器肩负着 Active Directory 核心功能。Active Directory 域中有 5 种类型的操作主机，分别是：

- 架构主机(Schema Master)。
- 域命名主机(Domain Naming Master)。
- PDC 仿真器(PDC Emulator)。
- RID 主机(RID Master)。
- 基础架构主机(Infrastructure Master)。

其中，每个林中必须具备一个架构主机和一个域命名主机两种操作主机，并且这些角色是唯一的。而在林的每个域中都必须具备 RID 主机、PDC 主机和基础架构主机，并且均是唯一的。

1. 操作主机的重要性

操作主机在 Active Directory 环境中，肩负着重要的作用，如果操作主机出现故障，将会出现以下问题：

- 当架构主机不可用时，不能对架构进行更改。在大多数网络环境中，对架构更改的频率很低，并且应提前进行规划，以免由于架构主机的故障，导致网络功能受到影响。
- 当域命名主机不可用时，不能通过运行 DCPROMO 向活动目录中添加或删除域，如果强行操作，将会收到类似“RPC 服务器不可用”的提示信息。
- 当 RID 主机不可用时，所遇到的主要问题是不能向域中添加任何新的安全对象，例如用户、组和

计算机。

- 当 PDC 主机不可用时，在本机模式环境中用户登录失败的可能性增大。
- 当基础架构主机不可用时，结构主机故障对环境的影响是有限的。最终用户并不能感觉到它的影响，只会对管理员执行大量组操作产生影响。这些组操作通常是添加用户/或重新命名用户。在此情况下，结构主机故障只是会延迟通过 Active Directory 管理单元引用这些更改的时间。

2. 安全规划

鉴于操作主机在域中担负着如此重要的作用，转移或更改之前必须做好细致的规划。

(1) 单域环境

Windows Server 2003/2008 单域控制器上角色的初始配置，只能将所有 FSMO 主机角色规划部署在一台 Windows Server 2003/2008 域控制器上。全局编录服务器也配置在此服务器上。在活动目录森林里只有一个域的情况下，基础架构主机是不起作用的。

(2) 多域环境

在多域环境中，存在多台域控制器和多台全局编录服务器，对性能的要求如下。

- 具有架构主机角色的域控制器上不需要高性能，通常情况下，只需保证其可用性即可，很少用于实际扩展。
- 具有域命名主机角色的域控制器不需要高性能，但是要保证高可用性。
- 具有 PDC 主机角色的域控制器是 FSMO 五种角色里任务最重的，占用 PDC 模拟器的域控制器要保证高性能和高可用性。
- 具有 RID 主机角色的域控制器，不要求高性能，但要保证高可用性。
- 具有基础架构主机角色的域控制器，可忽略性能和高可用性。

可以根据如下规则规划 FSMO 角色。

- 备用服务器与主要 FSMO 服务器位于同一站点中，以便在大的计算机组中获得更快的复制性能。
- 将 RID 角色和 PDC 模拟器角色放置在同一域控制器上。因为下级客户端和应用程序以 PDC 为目标，所以应保证从 PDC 到 RID 主机的良好通信。
- 在目录林级别上，架构主机角色和域命名主机角色应该放置在同一域控制器上。另外，域命名主机 FSMO 也应该是全局目录服务器。
- PDC 主机建议单独规划在一台域控制器上。
- 域命名主机和全局编录服务器规划在一台域控制器上。
- 使用一个管理控制台可管理所有的 FSMO 角色，并且确认所有的 FSMO 都是正常的。

“不要将结构主机放在全局目录服务器上”这一规则有以下两个例外。

- 单域目录林：在包含单个 Active Directory 域的目录林中没有跨域操作，因此没有需要结构主机完成的任务。在这种情况下，可以将结构主机放在域中的任一域控制器上。
- 多域目录林：其中的每个域控制器都包含全局目录，如果目录林中的每个域控制器承载全局目录，则没有需要结构主机完成的任务。在这种情况下，可以将结构主机放在目录林中的任一域控制器上。

3. 转移操作主机

在 Active Directory 环境中，如果具备操作主机角色的域控制器出现故障，在域控制器可用的情况下，

可以使用“转移角色”的方式完成操作主机角色的转移。在域控制器不可用的情况下，可以使用“占用角色”的方式完成操作主机角色的转移。角色转移过程是可逆的，既可以从 A 域控制器转移到 B 域控制器，也可以从 B 域控制器重新转移到 A 域控制器。

这里以域 coolpen.net 为例，介绍如何将操作主机角色从主域控制器(liuxh.coolpen.net)转移到额外域控制器(tianjl.coolpen.net)，主要操作包括：

- 转移“Active Directory 用户和计算机”中的操作主机角色。
- 转移“Active Directory 域和信任关系”中的操作主机角色。
- 转移“Active Directory 架构”中的操作主机角色。

(1) 转移“Active Directory 用户和计算机”中的操作主机角色

① 在主域控制器上，依次单击选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，将操作主机转移到额外域控制器之前，必须先连接到额外域控制器，即右击 coolpen.net 并选择快捷菜单中的“更改域控制器”命令，如图 3-4 所示。

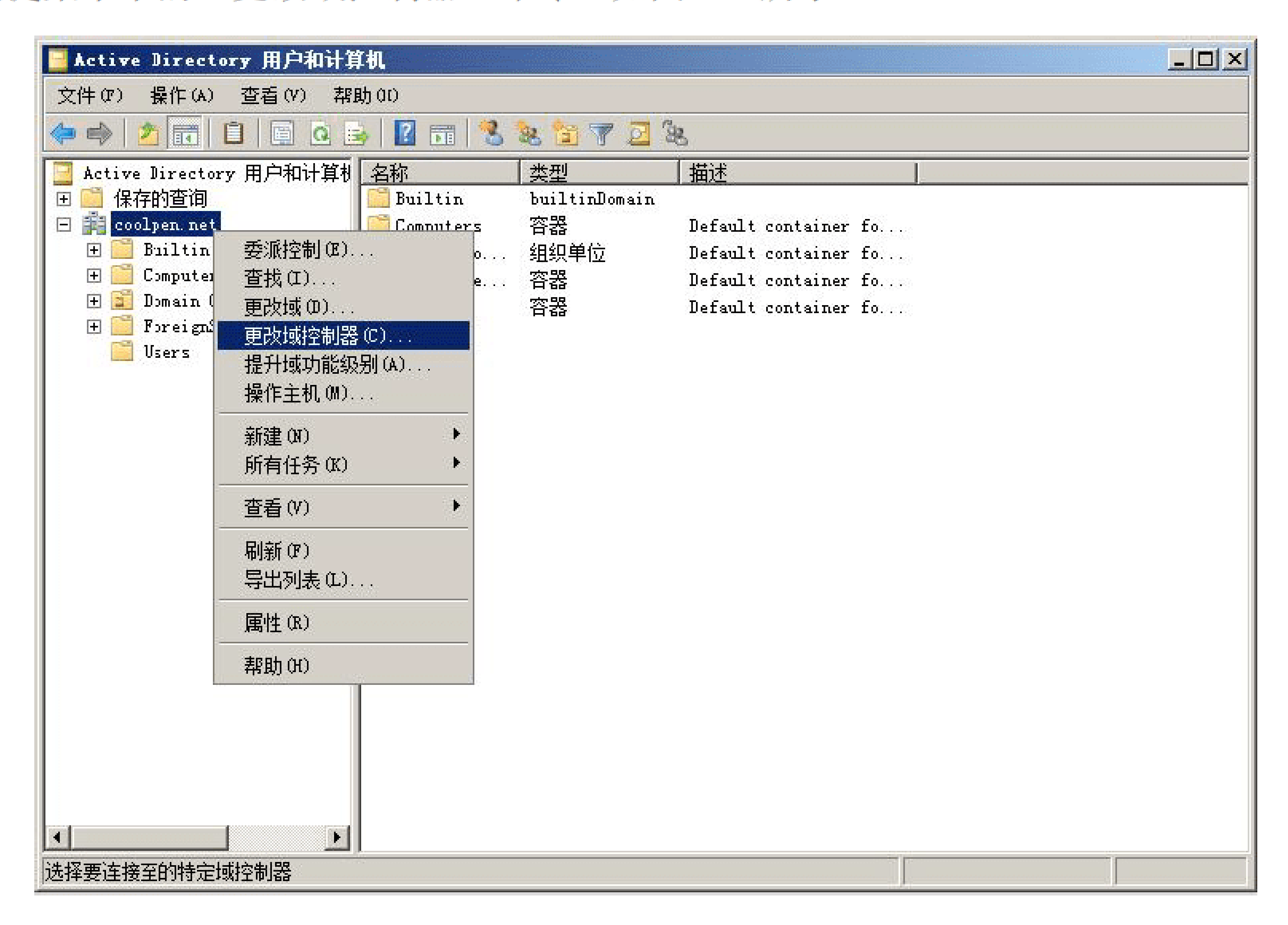


图 3-4　连接到额外域控制器

② 打开如图 3-5 所示的“更改目录服务器”对话框，选择“此域控制器或 AD LDS 实例”单选按钮，选中 tianjl.coolpen.net，也可以选中“在此处键入目录服务器名称[:端口]”，输入域控制器或轻型目录服务器实例所在服务器的 IP 地址和端口号。

③ 单击“确定”按钮，返回到“Active Directory 用户和计算机”窗口。

④ 继续在主域控制器上右击 coolpen.net，选择快捷菜单中的“操作主机”命令，显示如图 3-6 所示的“操作主机”对话框，默认显示 RID 选项卡。“操作主机”文本框中显示原主域控制器的主机名。

⑤ 单击“更改”按钮，显示如图 3-7 所示的“Active Directory 域服务”对话框，即可将更改 RID 主机角色转移到额外域控制器上。

⑥ 单击“是”按钮，确认转移操作主机角色，显示如图 3-8 所示的“Active Directory 域服务”对话框，提示“成功传送了操作主机角色”。



图 3-5　“更改目录服务器”对话框

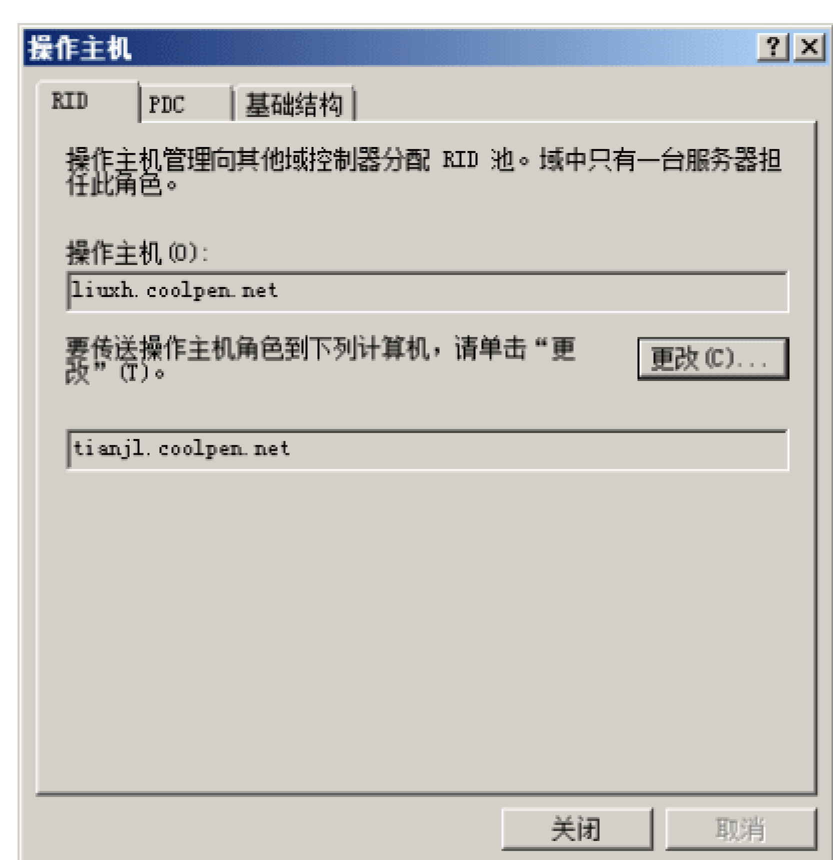


图 3-6　RID 选项卡




图 3-7　“Active Directory 域服务”对话框　　图 3-8　“Active Directory 域服务”对话框

⑦ 单击“确定”按钮，返回到“操作主机”对话框的 RID 选项卡，如图 3-9 所示，“操作主机”文本框中已经转变为额外域控制器的主机名。

⑧ 使用相同的方法在 PDC 选项卡中，将“操作主机”由原来的“liuxh.coolpen.net”更改为“tianjl.coolpen.net”，如图 3-10 所示。

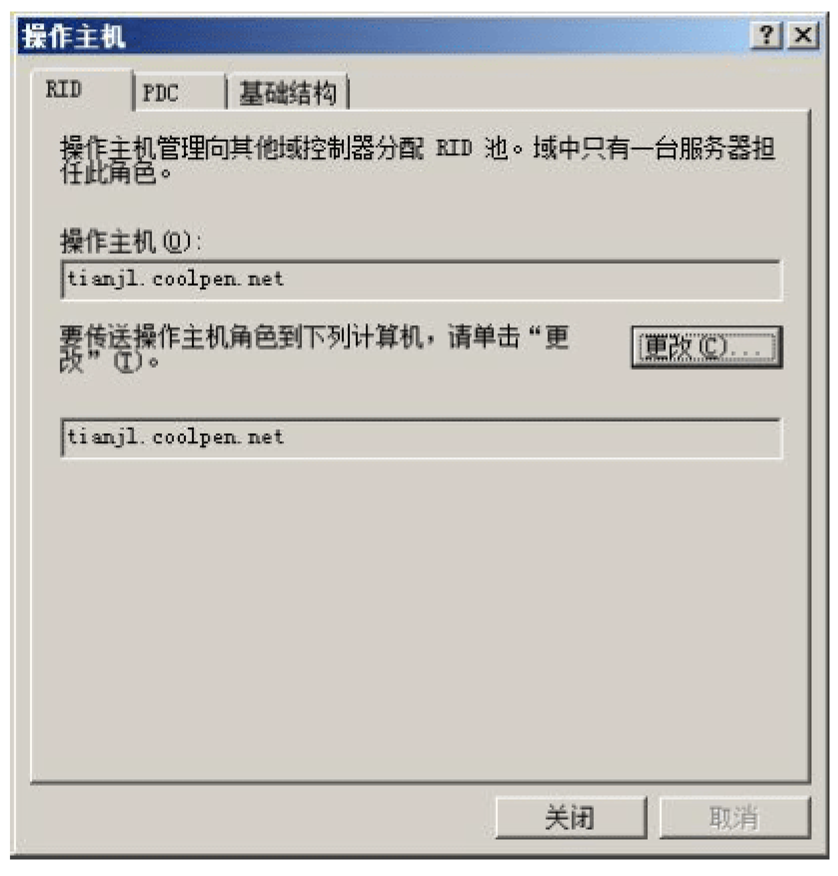
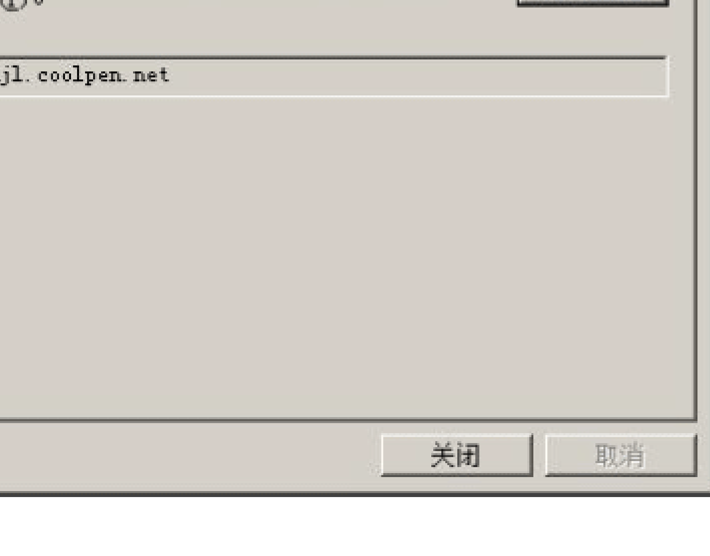



图 3-9　成功转移 RID 操作主机

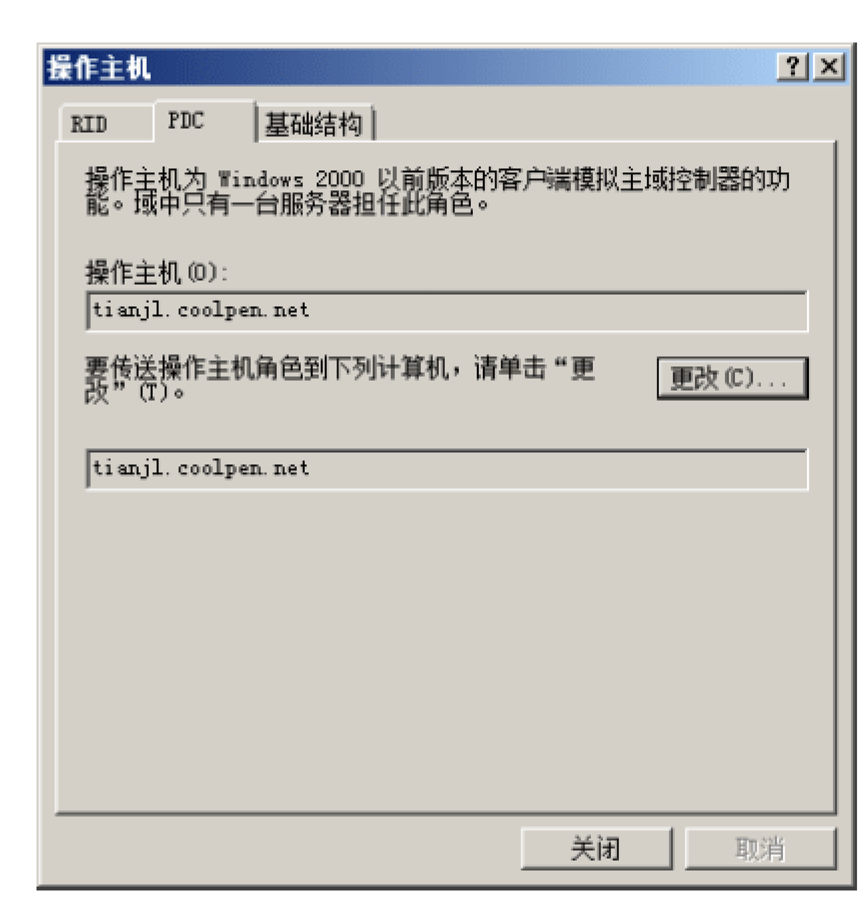


图 3-10　成功转移 PDC 操作主机

⑨ 使用相同的方法，在“基础结构”选项卡中将“操作主机”由原来的“liuxh.coolpen.net”更改为“tianjl.coolpen.net”，如图 3-11 所示。

注意：“基础结构”角色的转移与当前额外域控制器是否同时担当“全局编录”角色有关，如果是则将提示如图 3-12 所示的“Active Directory 域服务”对话框。但此时如果可以确保额外域控制器上“全局编录”服务的可用性，也可以单击“是”按钮强行转移。强行转移此角色并不会对其他角色的功能产生影响。

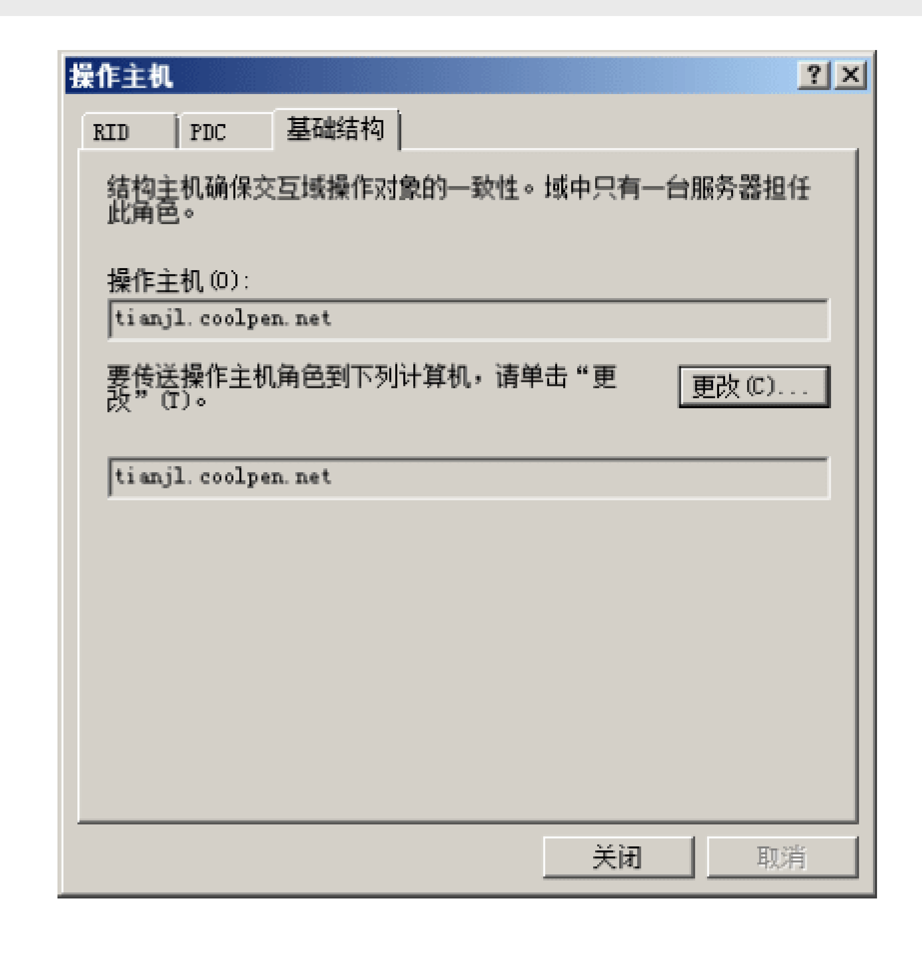


图 3-11 “基础结构”选项卡

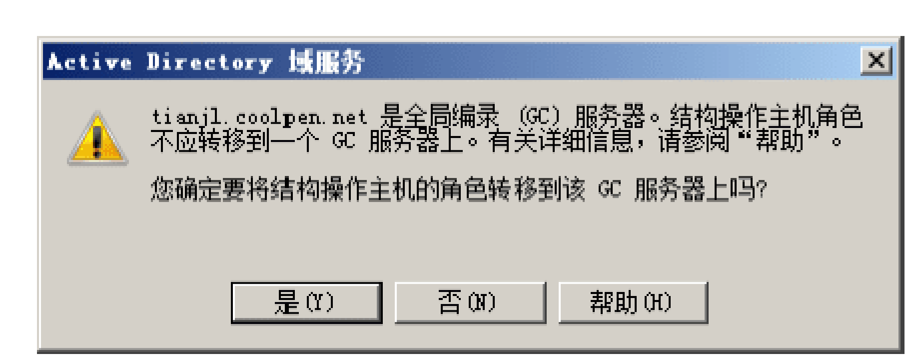


图 3-12 “Active Directory 域服务”对话框

(2) 转移“Active Directory 域和信任关系”中的操作主机角色

① 在主域控制器上，依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，打开如图 3-13 所示的窗口。

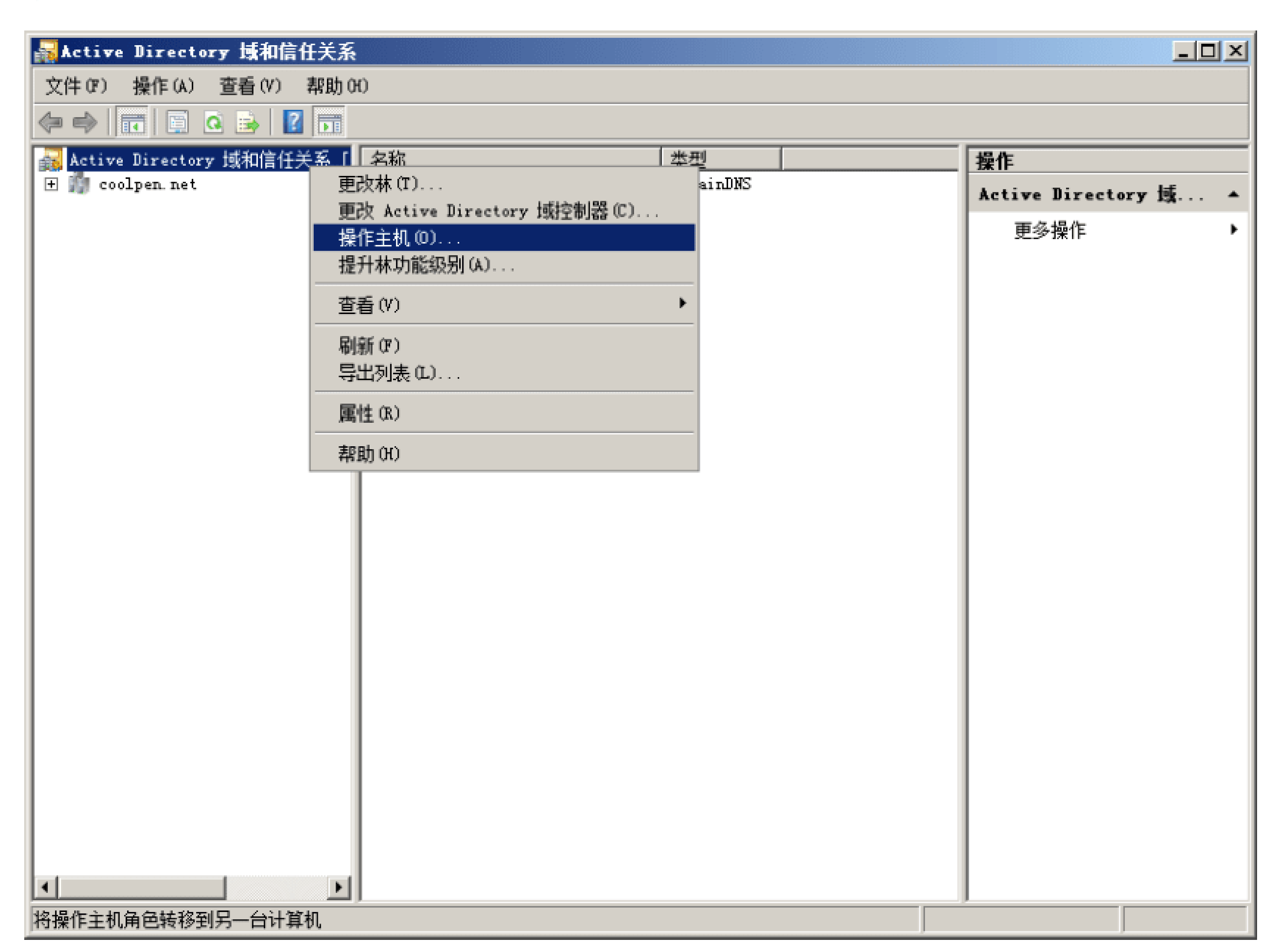


图 3-13 “Active Directory 域和信任关系”窗口

② 右击“Active Directory 域和信任关系”，选择快捷菜单中的“操作主机”命令，显示如图 3-14 所示的“操作主机”对话框。“域命名操作主机”默认仍是原来的主域控制器名称。

③ 单击“更改”按钮，显示如图 3-15 所示的“Active Directory 域和信任关系”对话框。



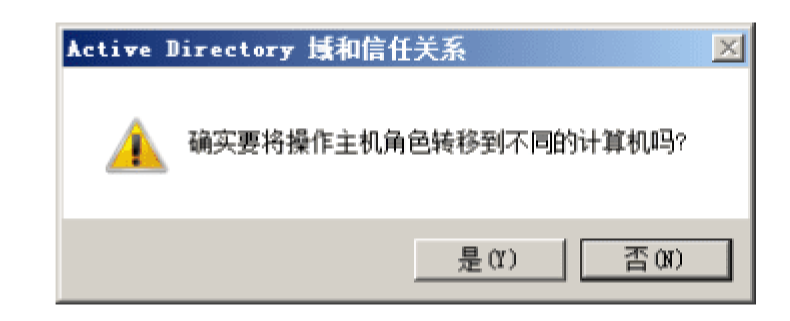


图 3-14　“操作主机”对话框　　　　图 3-15　“Active Directory 域和信任关系”对话框

④ 单击“是”按钮确认，即可成功转移域命名主机，显示如图 3-16 所示的结果。

(3) 转移“Active Directory 架构”中的操作主机角色

在 Windows Server 2003/2008 域中，默认情况下并没有将 Active Directory 架构注册到系统中，因此进行架构查看和操作之前，必须先进行注册。转移“Active Directory 架构”中的操作主机角色的主要操作步骤如下。

① 在主域控制器上，单击“开始”按钮，在“开始搜索”文本框中，输入 regsvr32 schmmgmt.dll 并按 Enter 键，在系统中注册 schmmgmt.dll 组件，成功后显示如图 3-17 所示的对话框。直接单击“确定”按钮关闭即可。






图 3-16　成功转移域命名角色　　　　图 3-17　注册 schmmgmt.dll 组件

② 在“开始”菜单的“开始搜索”文本框中输入“MMC”并按 Enter 键，打开如图 3-18 所示的“控制台”窗口，为了便于管理，可以借助这种方法将注册成功的“Active Directory 架构”添加到控制台中。

③ 依次选择“文件”→“添加/删除管理单元”命令，打开“添加或删除管理单元”对话框，在“可用的管理单元”列表中选择“Active Directory 架构”组件，并单击“添加”按钮将其添加到“所选管理单元”列表中，如图 3-19 所示。注册 schmmgmt.dll 组件之前，是不会出现该组件的。

④ 单击“确定”按钮保存设置并退出，显示如图 3-20 所示的窗口，即可看到成功添加到控制台中的“Active Directory 架构”管理单元。

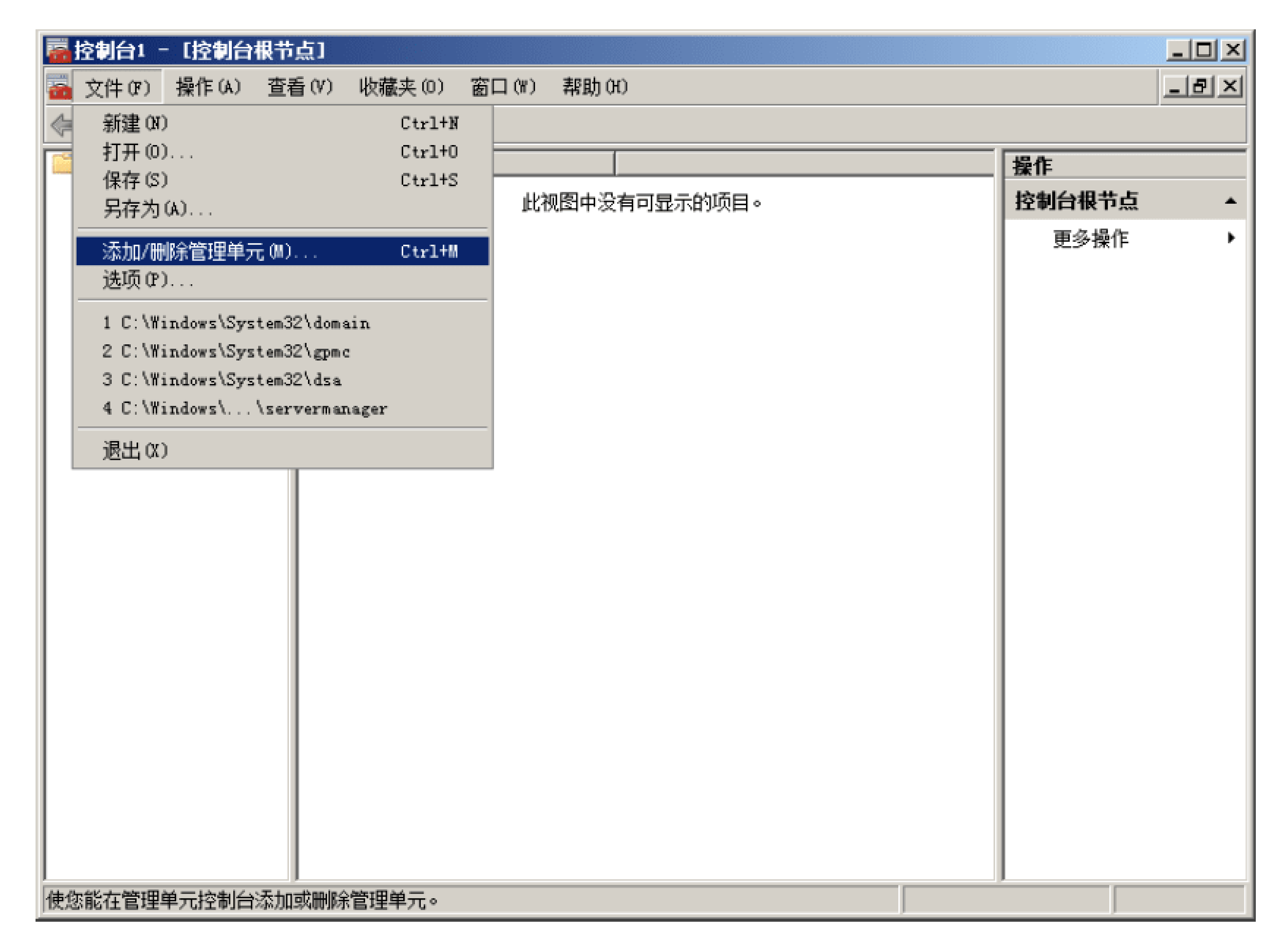


图 3-18 “控制台”窗口

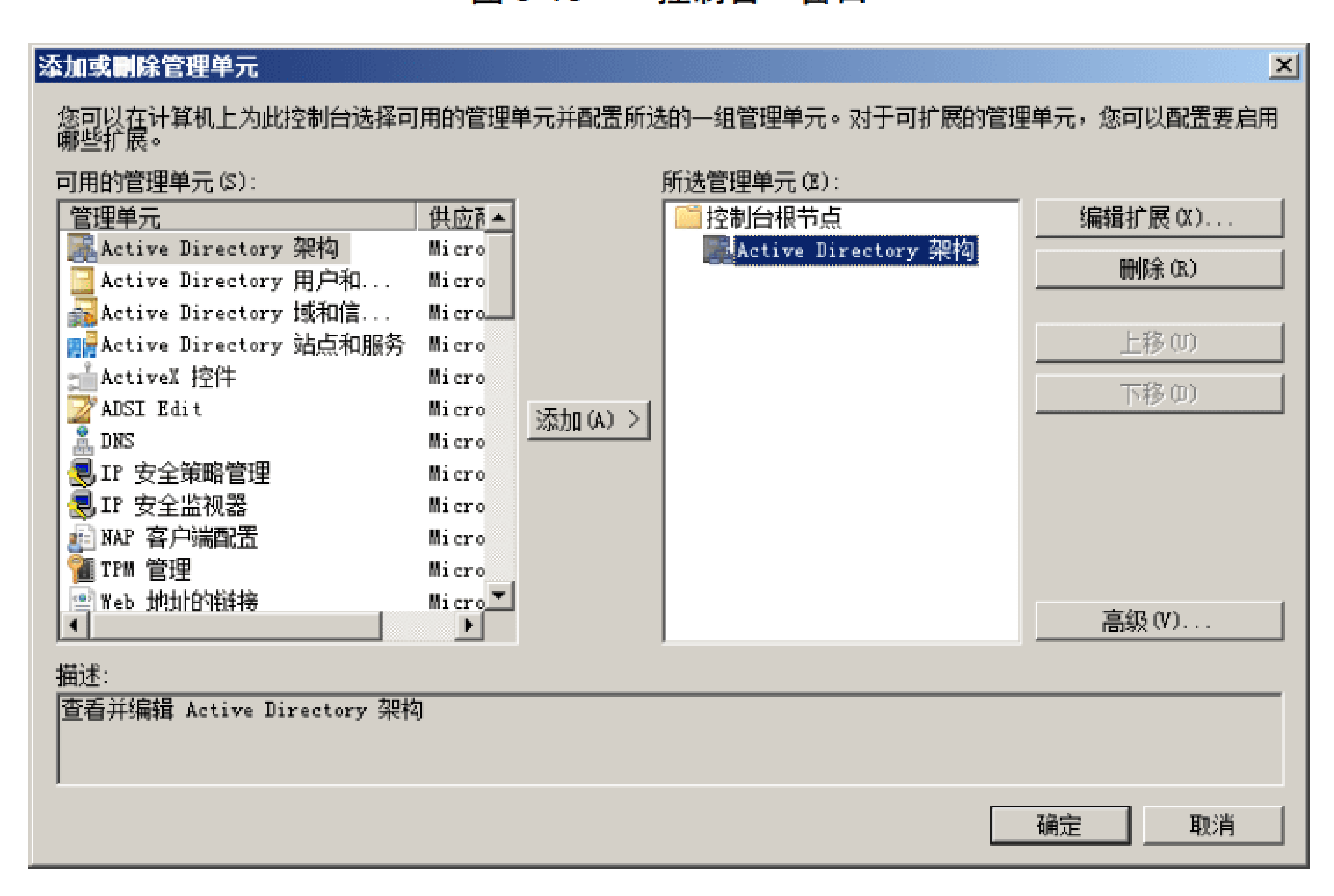


图 3-19 “添加或删除管理单元”对话框

⑤ 右击“Active Directory 架构”，选择快捷菜单中的“更改 Active Directory 域控制器”选项，显示如图 3-21 所示的“更改目录服务器”对话框。选择“此域控制器或 AD LDS 实例”单选按钮，并单击“tianjl.coolpen.net(额外域控制器计算机名称)”。单击“确定”按钮连接到额外域控制器。

⑥ 再次右击“Active Directory 架构”，选择快捷菜单中的“操作主机”命令，显示如图 3-22 所示的“更改架构主机”对话框。

⑦ 单击“更改”按钮，完成更改架构主机的转移。

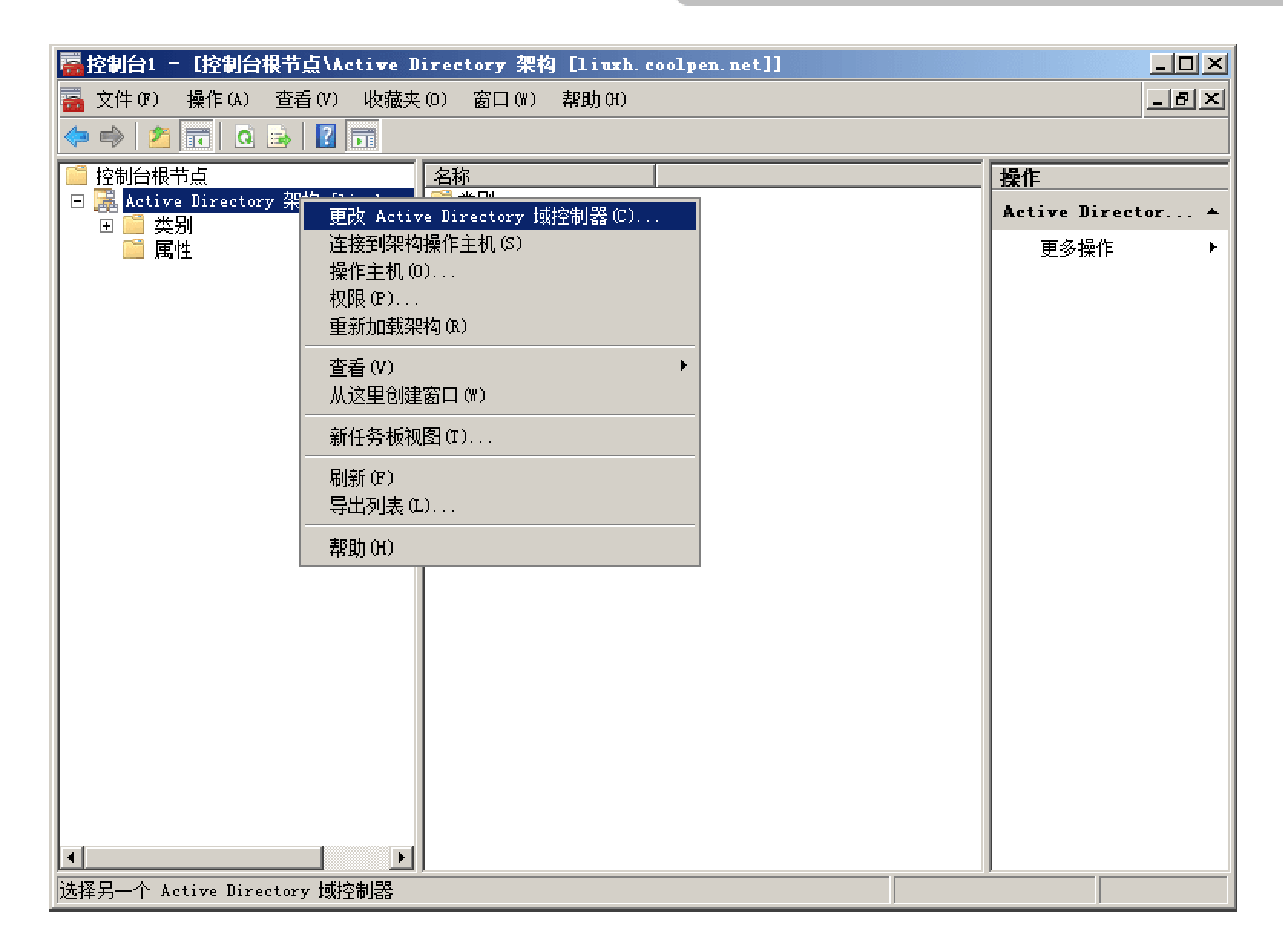


图 3-20　“Active Directory 架构”被添加到控制台中

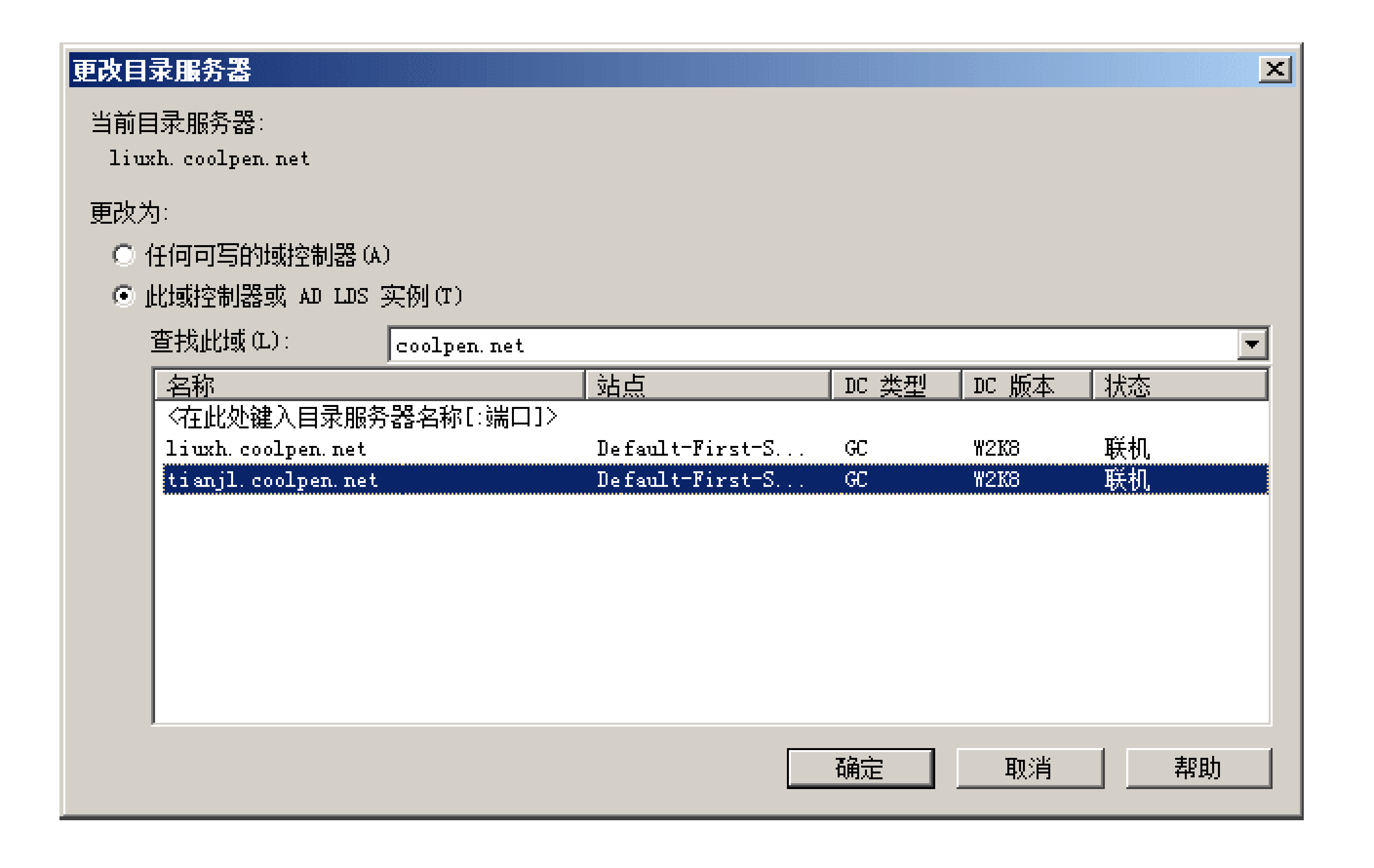


图 3-21　“更改目录服务器”对话框



图 3-22　“更改架构主机”对话框

3.1.3　功能级别

在 Windows Server 2008 域环境中，域功能级别的设置将直接影响本地域控制器的兼容范围和功能扩展，但不会影响到同一目录林中的其他域。Windows Server 2008 Active Directory 域共有 3 种域功能级别可供选择。

- Windows 2000 混合模式：类似于 Windows 2000 Active Directory 的“混合模式”，可以兼容 Windows 2000 Server、Windows NT Server 和 Windows Server 2003 域控制器。
- Windows Server 2003：只能运行兼容 Windows Server 2003 域服务器，但可以享受 Windows Server 2003 Active Directory 域所提供的完整特性和功能，以及 Windows 2000 混合模式的域

功能。

- Windows Server 2008：可以提供所有默认的 Active Directory 功能，兼容 Windows Server 2003 域服务器功能，这是 Windows 域的最高功能级别。

1. 域功能级别提升

默认状态下，无论是 Windows Server 2003 还是 Windows Server 2008 域的功能级别都是 Windows 2000 混合模式，这主要是为了兼容网络中早期版本的 Windows 用户。随着网络中计算机系统的不断升级，可以根据需要提升域控制器的功能级别，以获得更多的功能支持。将 Windows Server 2008 域功能级别从 Windows 2000 混合模式提升为 Windows Server 2003 模式，主要操作步骤如下。

① 依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，显示“Active Directory 用户和计算机”窗口，如图 3-23 所示。

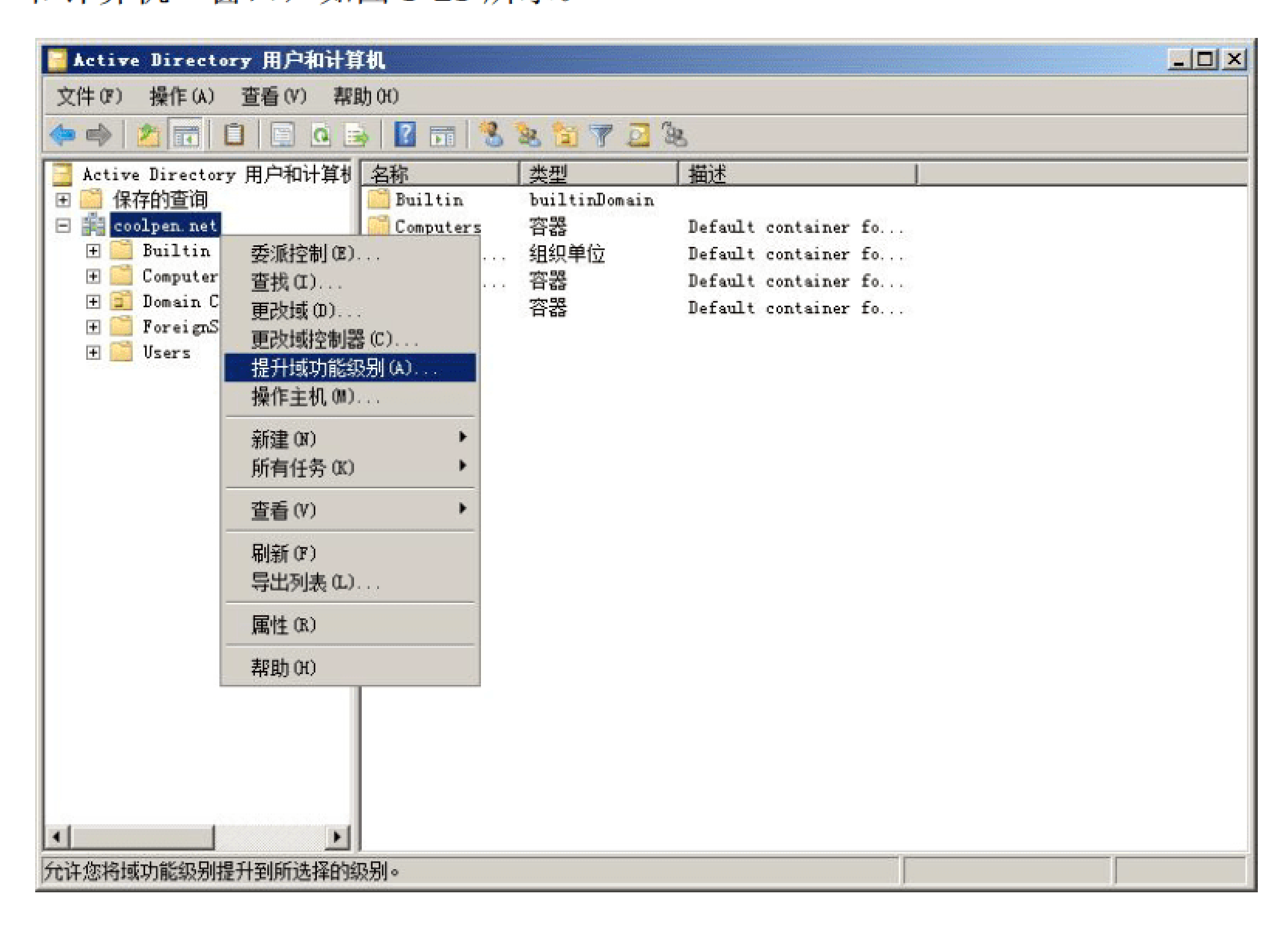


图 3-23 “Active Directory 用户和计算机”窗口

② 右击域名 coolpen.net，选择快捷菜单中的“提升域功能级别”命令，出现如图 3-24 所示的“提升域功能级别”对话框，在“选择一个可用的域功能级别”下拉列表框中，选择 Windows Server 2003 选项。由于当前级别模式为 Windows 2000 纯模式，所以只能选择 Windows Server 2003 或 Windows Server 2008。



图 3-24 “提升域功能级别”对话框

③ 单击“提升”按钮，显示如图 3-25 所示的“提升域功能级别”对话框。

④ 单击“确定”按钮，开始提升域 coolpen.net 的功能级别，提升完成显示如图 3-26 所示的“提升域功能级别”信息提示框。

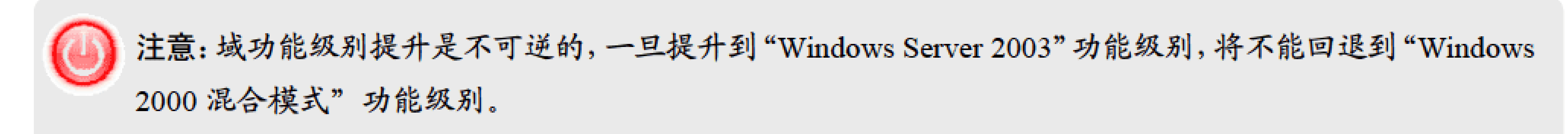


图 3-25　“提升域功能级别”对话框



图 3-26　“提升域功能级别”信息提示框

⑤　单击“确定”按钮，完成域功能级别的提升。



注意：域功能级别提升是不可逆的，一旦提升到“Windows Server 2003”功能级别，将不能回退到“Windows 2000 混合模式”功能级别。

2. 林功能级别提升

域林功能用于决定林中可以被激活的功能种类。Windows Active Directory 林功能可分为如下 3 种级别。

- Windows 2000：该功能级别与默认设置下的“Windows 2000 域级别”类似，是系统默认的目录林功能级别，只能提供最基础的目录林结构特性与功能。
- Windows Server 2003：该功能级别的目录林允许使用全部的目录林特性和功能，但只能与 Windows Server 2003 域兼容。
- Windows Server 2008：Windows Server 2003 林功能级别上可用的所有功能，但在默认情况下，随后添加到林的所有域将在 Windows Server 2008 域功能级别下进行操作。

默认状态下，Windows 目录林功能级别使用的是 Windows 2000 混合模式，如果要提升到 Windows Server 2003 或 Windows Server 2008 林功能级别模式，必须先将网络的所有域控制器功能级别提升到 Windows Server 2003 或 Windows Server 2008。

①　依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，打开如图 3-27 所示的“Active Directory 域和信任关系”窗口。

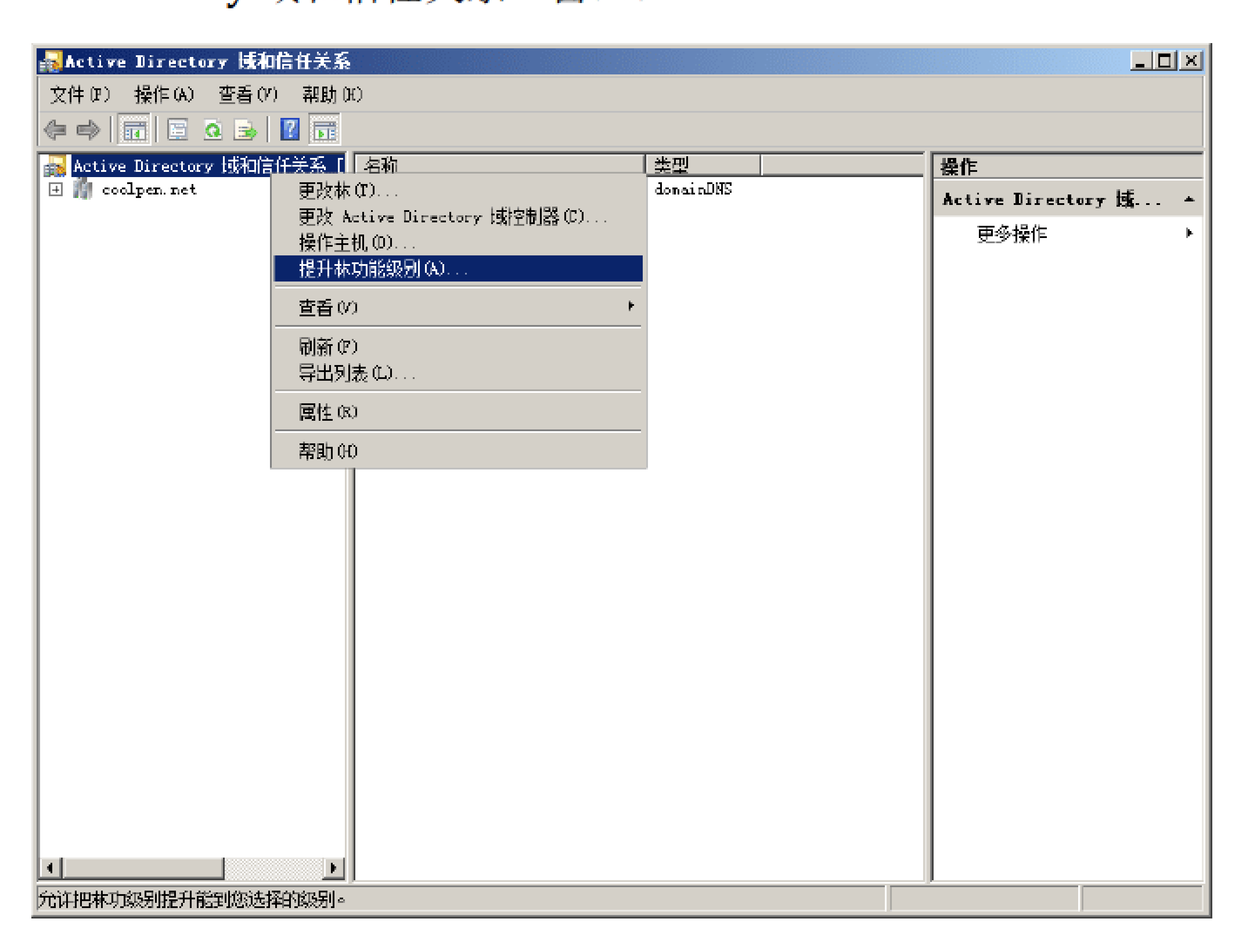


图 3-27　“Active Directory 域和信任关系”窗口

② 右击“Active Directory 域和信任关系”，选择快捷菜单中的“提升林功能级别”命令，显示如图 3-28 所示的“提升林功能级别”对话框。在“选择一个可用的林功能级别”下拉列表框中选择 Windows Server 2003 即可。

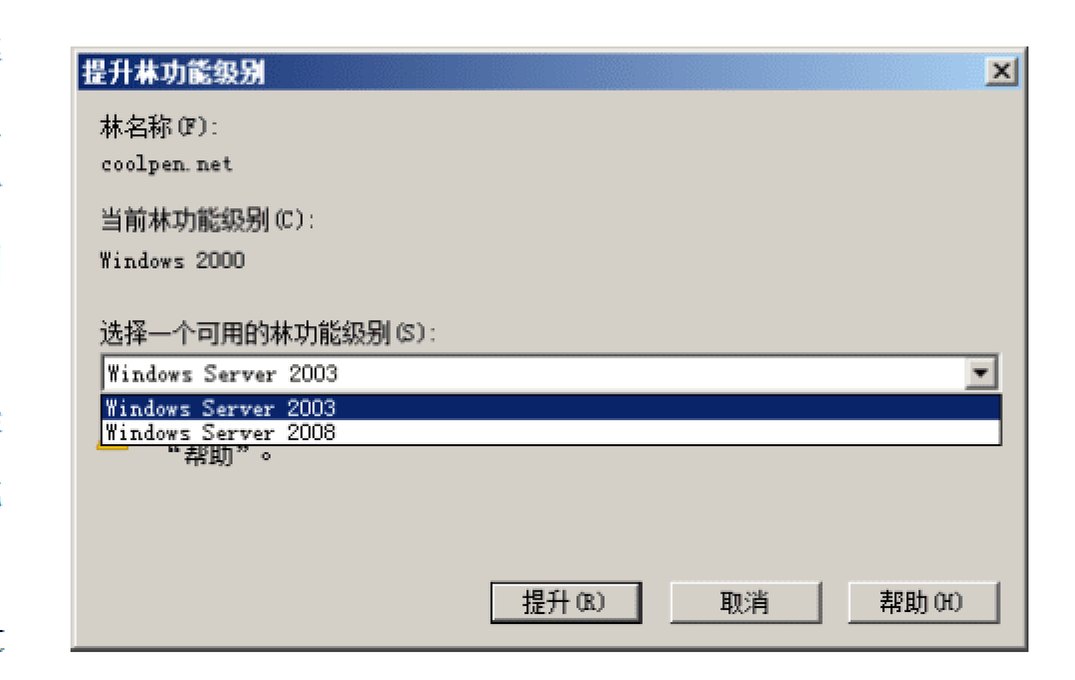


图 3-28 “提升林功能级别”对话框

③ 单击“提升”按钮，显示如图 3-29 所示的“提升林功能级别”对话框，提示该提升过程是无法还原的。

④ 单击“确定”按钮，开始提升目录林 coolpen.net 的功能级别，提升完成后显示如图 3-30 所示的“提升林功能级别”信息提示框。提示操作成功，并会将新的林功能级别复制到林中的每台域控制器上。



图 3-29 确认提升

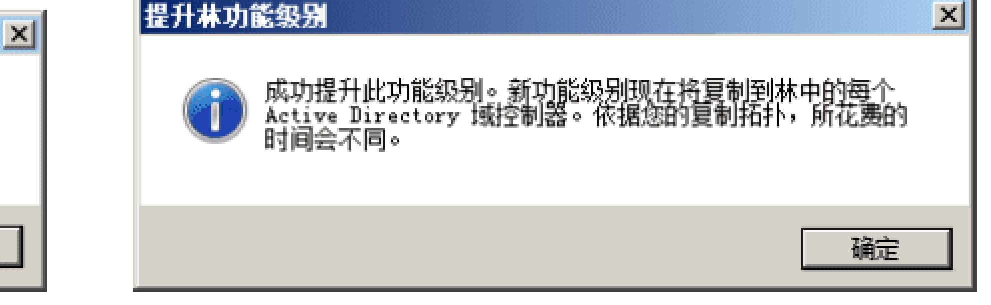


图 3-30 “提升林功能级别”信息提示框

⑤ 单击“确定”按钮关闭对话框，完成目录林功能提升操作。



注意： Windows 2000 纯模式和 Windows 2000 混合模式是完全不同的域功能级别，Windows Server 2003 的域控制器安装时可以任选其中一种模式，但在安装 Windows Server 2008 域过程中只能选择 Windows 2000 纯模式。网络中同时包含 Windows Server 2003 域控制器和 Windows Server 2008 域控制器的用户，提升林功能级别时应注意做好协调工作。

3.1.4 信任关系

域是网络中的安全边界，通常情况下不存在任何联系的域之间，是无法实现资源共享的。信任关系就是建立在域之间的逻辑关系，是彼此之间实现资源共享及互访的重要前提。通过信任关系的建立，可以将彼此的对象信息以某种方式相互传递，使分布于不同域的用户可以实现跨域登录。

1. 信任传递性

信任关系的传递性决定信任关系是否可扩展到建立信任的两个域之外，按照是否具有可传递性，信任关系分为可传递信任和非传递信任。可传递信任用于将信任关系扩展到其他域，而非传递信任用于拒绝与其他域之间的信任关系。

(1) 可传递信任

任何一个 Windows Server 2008 或 Windows Server 2003 域被加入到域目录树后，这个域会自动信任其父域，同时父域也会自动信任这个新域，并且这些信任关系是可以传递到以后加入到目录树中的其他域的。可传递信任关系将以域树形成时的方向沿域树向上流动，最终在域树中的所有域之间创建可传递信任。如图 3-31 所示是可传递信任关系及访问示意图。

由于这种信任关系都是建立在父域和子域之间的，所以也被称为父子信任关系。除以这种方式默认创建的可传递信任关系外，还可以通过手动方式创建如下 3 种类型的可传递信任关系。

- 快捷信任：在相同域目录树或域目录林中的域之间的可传递信任，用于缩短大型复杂的域树或林中的信任路径。
- 林信任：在林根域和第 2 个林根域之间的可传递信任。
- 领域信任：在 Active Directory 域和 Kerberos V5 领域之间创建可传递信任。

(2) 非传递信任

非传递信任受信任关系中的两个域的约束，并不流向林中的任何其他域。此时用户也将无法访问到没有直接建立信任关系的域，如图 3-32 所示。

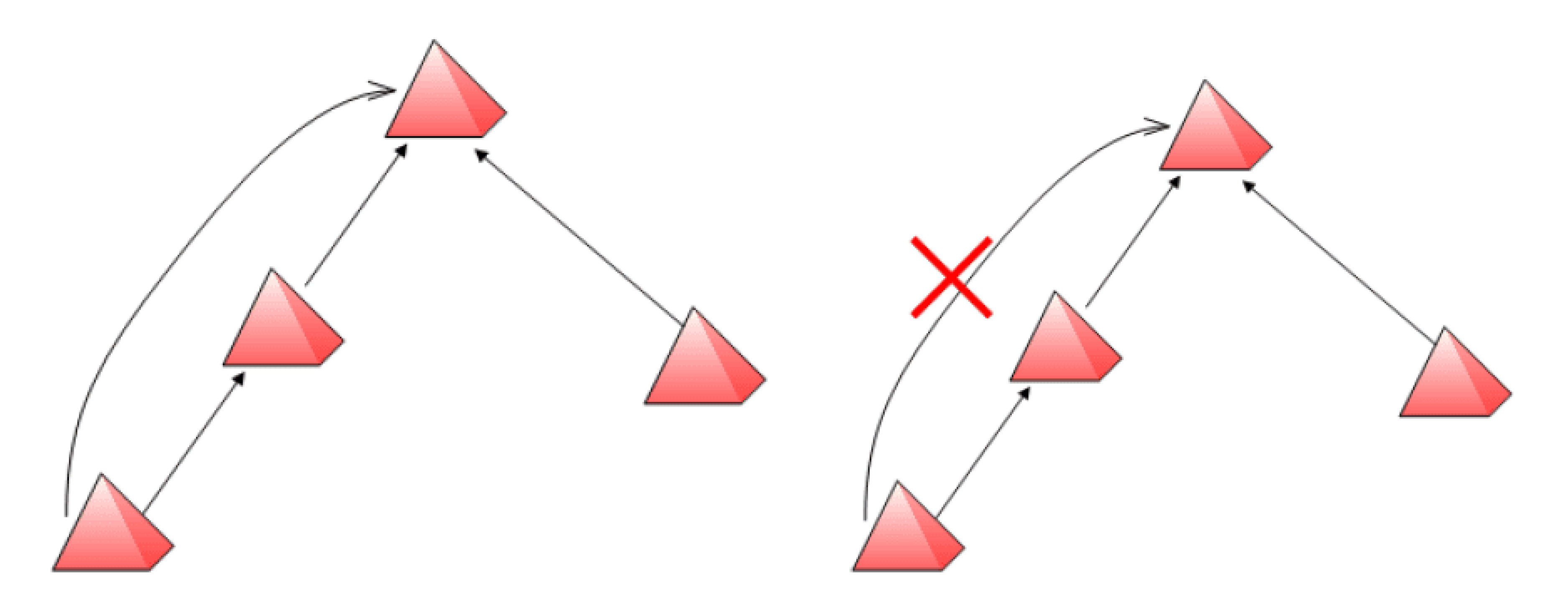


图 3-31 可传递信任关系　　图 3-32 非传递信任关系

非传递域信任是以下各项之间唯一的信任关系形式：

- Windows Server 2008 域、Windows Server 2003 域、Windows NT 域彼此之间。
- 一个林中的 Windows Server 2008 域和其他林中的某个域(当没有被林信任连接时)。

管理员可以使用手动方式创建下列非传递信任：

- 外部信任，在单个 Windows 域之间，或不同林的 Windows 域之间创建的非传递信任关系。
- 领域信任，在 Windows Active Directory 域和 Kerberos V5 领域之间的非传递信任。

2. 信任方向

“信任域”和“受信任域”是信任关系中的两个主体，信任方向就是决定彼此之间的信任方式，通常以箭头表示。信任方向的分配将直接影响到用于身份验证的路径，信任路径则是身份验证请求必须符合域之间的一系列信任关系。信任方向可以分为单向信任和双向信任。

(1) 单向信任

单向信任是两个域之间创建的单向身份验证路径，即受信任域中的用户账户可以使用信任域上的身份验证方式，并访问域中的资源，但反之则无法实现。如图 3-33 所示是单向信任关系示意图。

(2) 双向信任

默认情况下，Windows Server 2008 和 Windows Server 2003 林中的所有域信任关系都是双向、可传递的。创建新的子域时，双向可传递信任在新的子域和父域之间自动建立，这意味着身份验证请求可按两种方向在两个域之间传递。如图 3-34 所示为双向信任关系示意图。

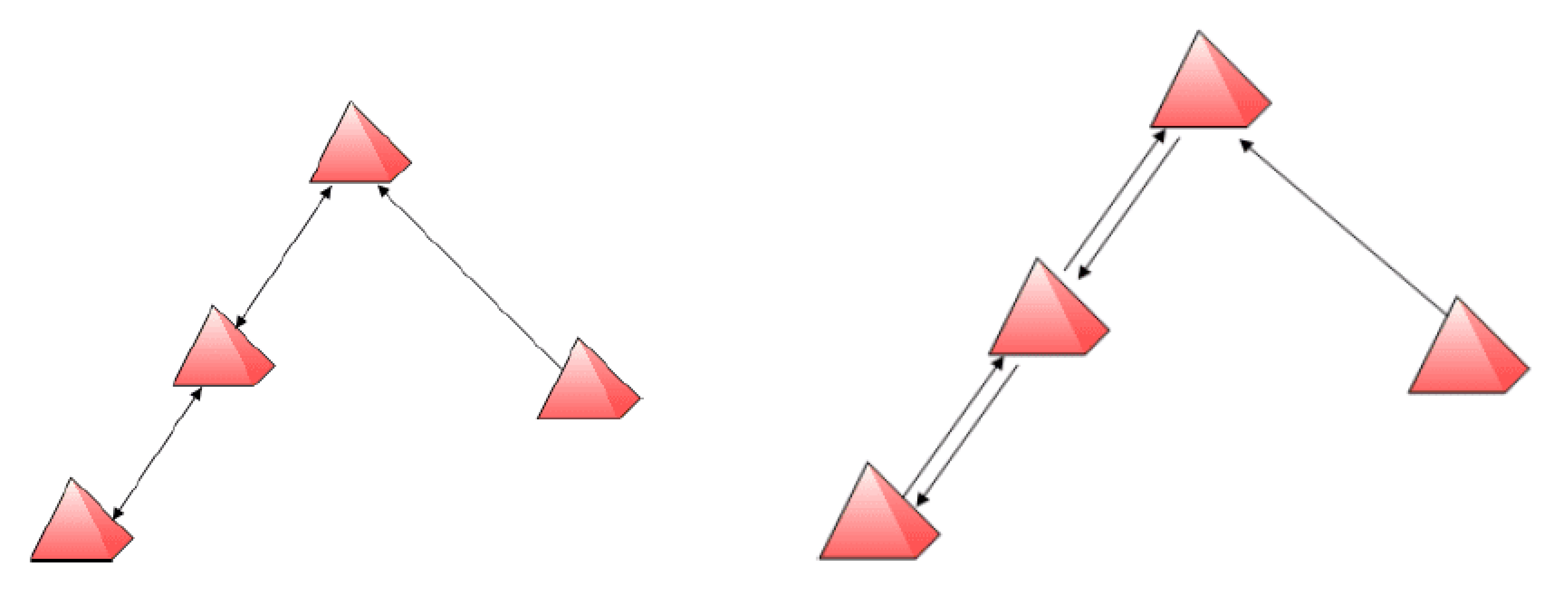


图 3-33 单向信任关系　　图 3-34 双向信任关系

Windows Server 2003 可以建立与下列各域之间的单向或双向信任：

- 同一林中的 Windows Server 2003 域。
- 不同林中的 Windows Server 2003 域。
- Windows NT 4.0 域。
- Kerberos V5 领域。

3. 信任安全规划

在默认状态下，在使用“Active Directory 安装向导”创建域的同时，系统会自动创建默认的信任关系、父子信任和域间信任。除此之外，用户根据需要创建信任关系之前，必须做好详细规划，以免实施之后导致不必要的网络安全威胁，通常应考虑如下因素。

(1) 何时创建快捷信任

快捷信任是当系统管理员需要优化身份验证过程时，可以使用单向或双向可传递信任。身份验证要求必须首先通过域树之间的信任路径，在复杂的林中，验证的时间会很长，执行的效率会很低。快捷信任可以缩短该信任验证的时间。信任路径是为了传递任何两个域之间的身份验证请求而必须遍历的一系列的域信任关系。

当某个域中经常有许多用户登录林中的其他域时，有必要使用快捷信任。快捷信任可有效地缩短在两个不同树中的域之间进行身份验证所要经过的路径。

- 使用单向信任：建立在不同域树中的两个域之间的单向快捷信任，可以减少完成身份验证请求所需的时间，但只能在一个方向上传递。
- 使用双向信任：建立在不同域树中的两个域之间的双向快捷信任，可以减少完成源自其中任一域的身份验证请求所需的时间。

(2) 何时创建林信任

只能在一个 Windows Active Directory 林的林根域和另一个 Windows Active Directory 林的林根域之间创建林信任，此时可以为目录林中的所有域控制器提供一种单向或双向的可传递信任关系。

- 使用单向林信任：两个林之间的单向林信任允许受信任林的成员使用信任林中的资源，但此信任只是单向的。
- 使用双向林信任：两个林之间的双向林信任允许任一个林的成员使用另一个林中的资源；每个林中的域隐式信任另一个林中的域。

4. 创建信任关系

创建信任关系可以帮助用户扩展网络应用范围，实现更广资源的集中管理和应用。当网络中有多个不同的域时，想要让每个用户可以自由地访问网络中的每台服务器(不管是否属于这个用户所属的域)时，这些域之间就需要创建信任关系。本案例的实验环境中包括两台彼此独立的主域控制器：coolpen.net 和 hsnc.cn，IP 地址分别为 192.168.1.21 和 192.168.1.25。

(1) 在其中一台域控制器(本例为 coolpen.net)上执行如下操作

① 依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，显示如图 3-35 所示的“Active Directory 域和信任关系”窗口。

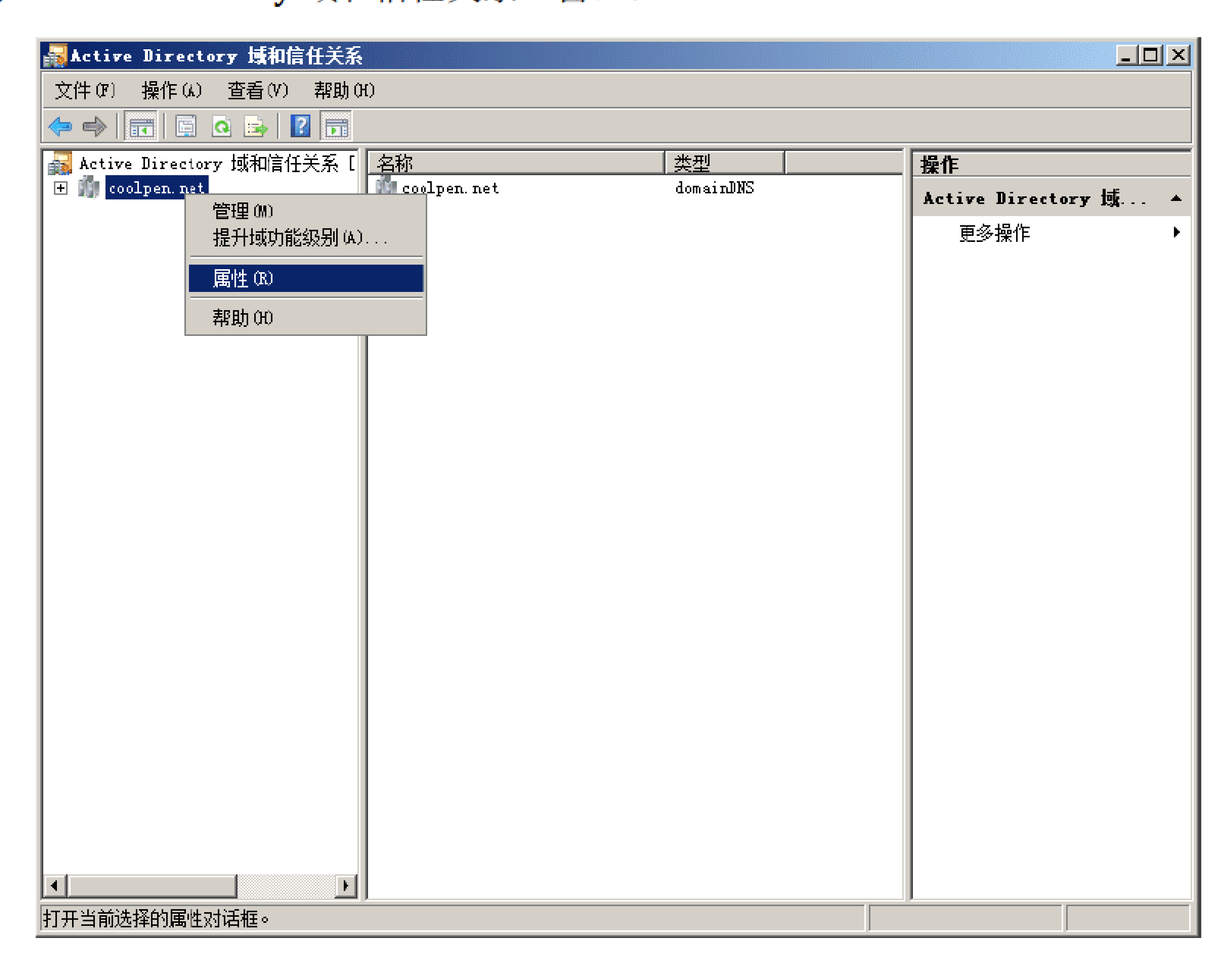


图 3-35　“Active Directory 域和信任关系”窗口

② 右击域名 coolpen.net，选择快捷菜单中的“属性”命令，打开“coolpen.net 属性”对话框，单击“信任”标签切换至如图 3-36 所示的“信任”选项卡。目前，该域中包含一个子域 hengshui.coolpen.net，自动创建了信任关系，所以显示在列表中。

③ 单击“新建信任”按钮，弹出“新建信任关系向导”对话框，如图 3-37 所示。

④ 单击“下一步”按钮，显示如图 3-38 所示的“信任名称”界面。在“名称”文本框中，输入想要与之建立信任关系的域控制器名称 hsnc.cn，也可以使用对方的 NetBIOS 名称 hsnc。

⑤ 单击“下一步”按钮，显示如图 3-39 所示的“信任方向”界面，可根据需要选择信任关系的方向，系统默认选择“双向”单选按钮。如果两台域控制器的功能和安全级别有所不同，建议选择单向信任。单向信任可以划分为“单向：内传”和“单向：外传”，分别表示该域中的用户可以在指定的域、领域、域林中得到身份验证，指定域、领域或域林的用户可以在该域中得到身份验证，这两种情况均是单向信任。

⑥ 单击“下一步”按钮，显示如图 3-40 所示的“信任方”界面。如果管理员具有每个域的相应管理权限，则可以通过选择“此域和指定的域”单选按钮，同时创建双方外部信任，否则选择“只是

这个域”单选按钮，由对方域控制器的管理员完成相应的操作即可。

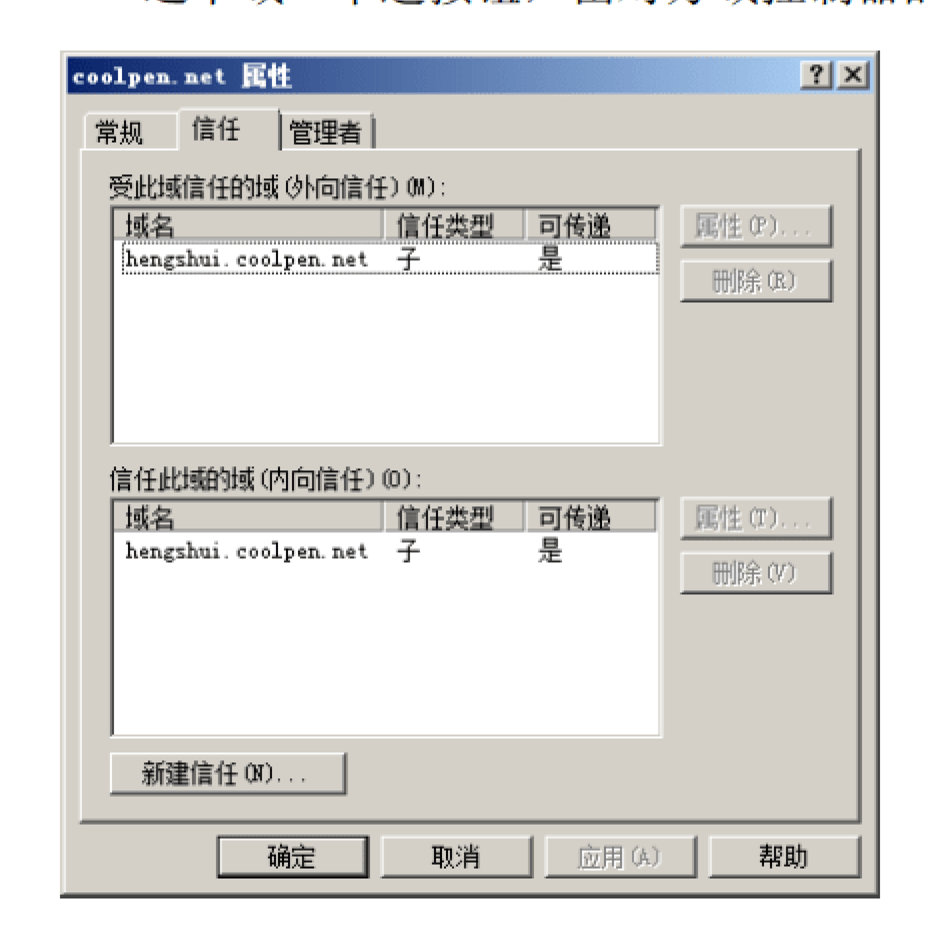


图 3-36　“信任”选项卡

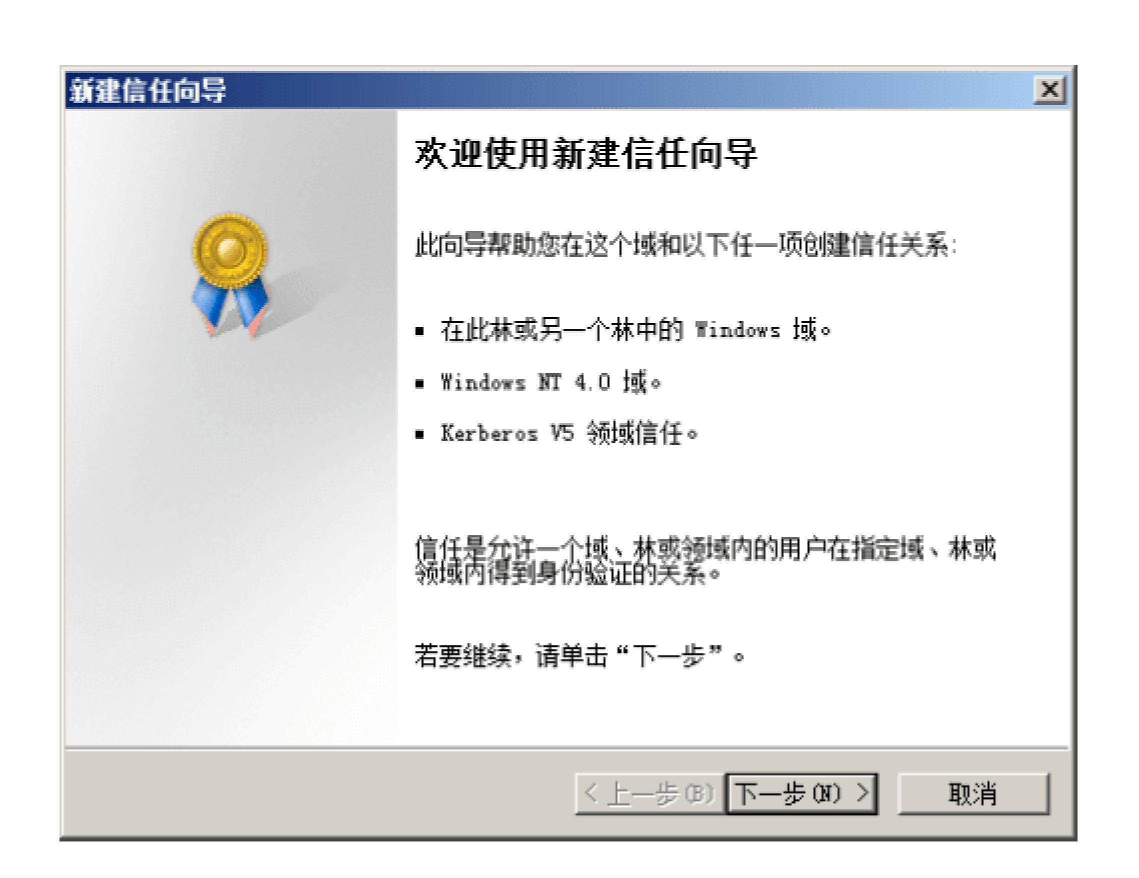


图 3-37　“新建信任向导”对话框

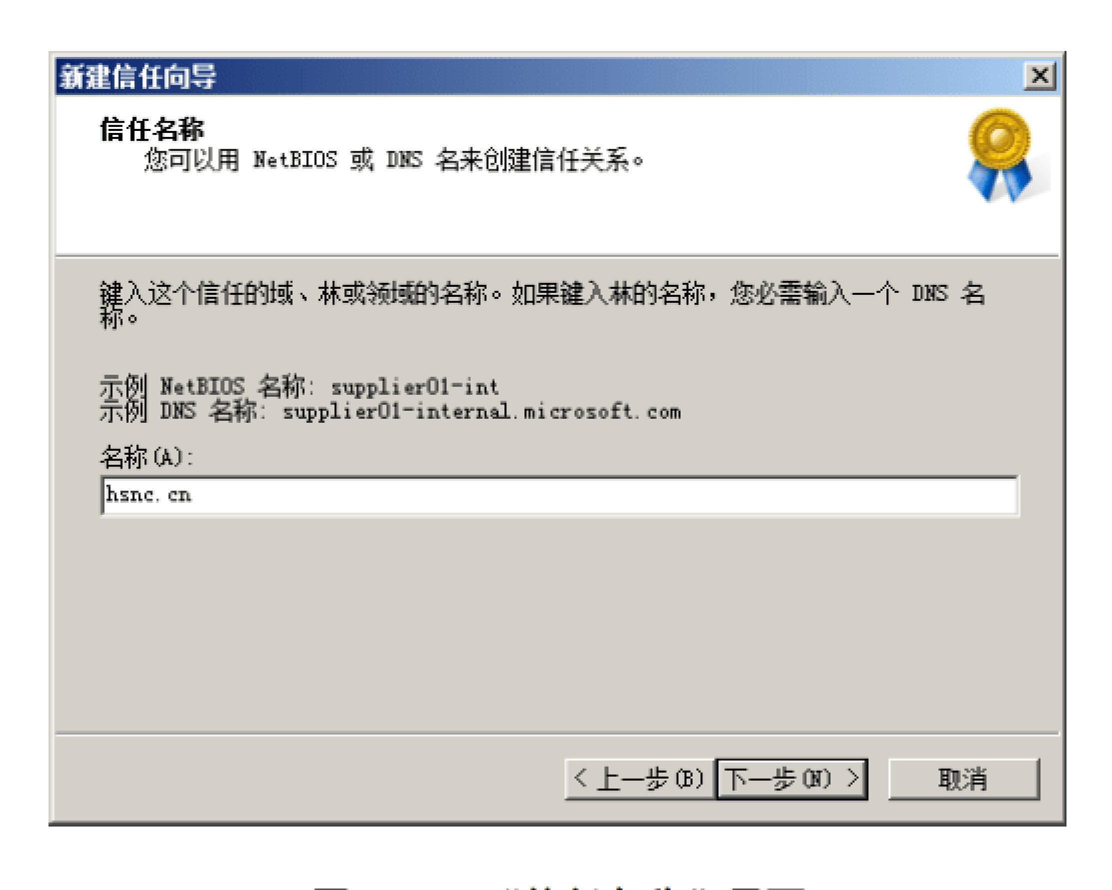


图 3-38　“信任名称”界面

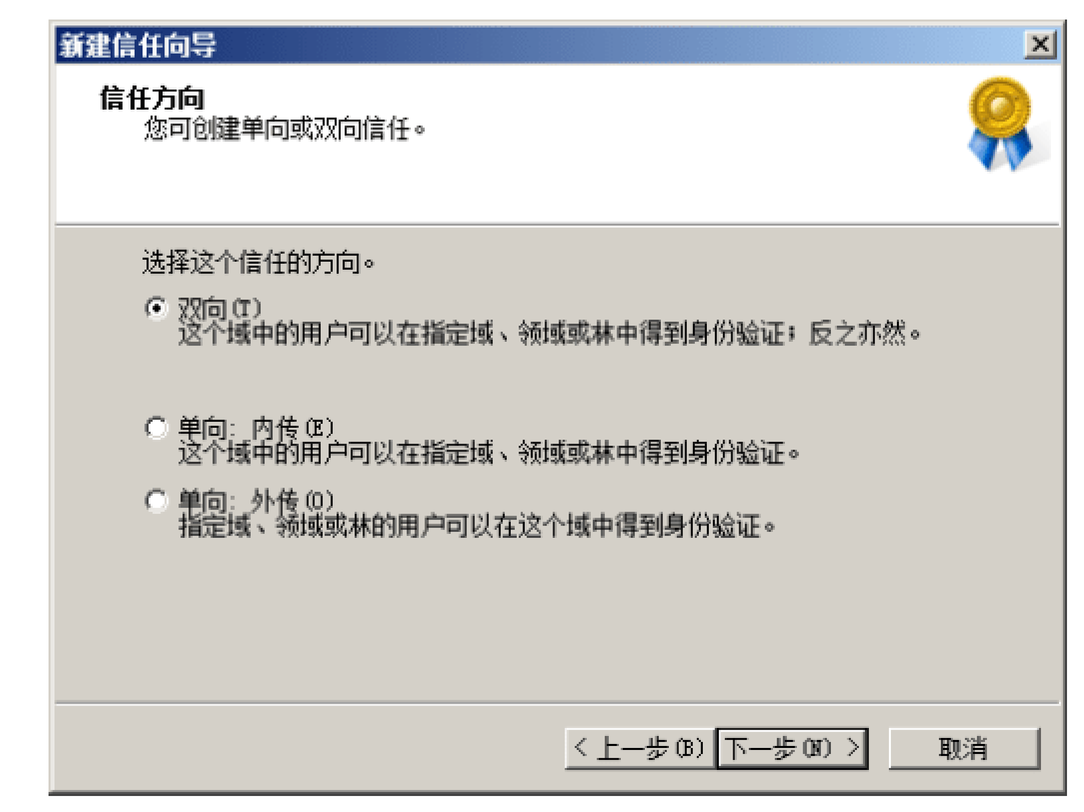


图 3-39　“信任方向”界面

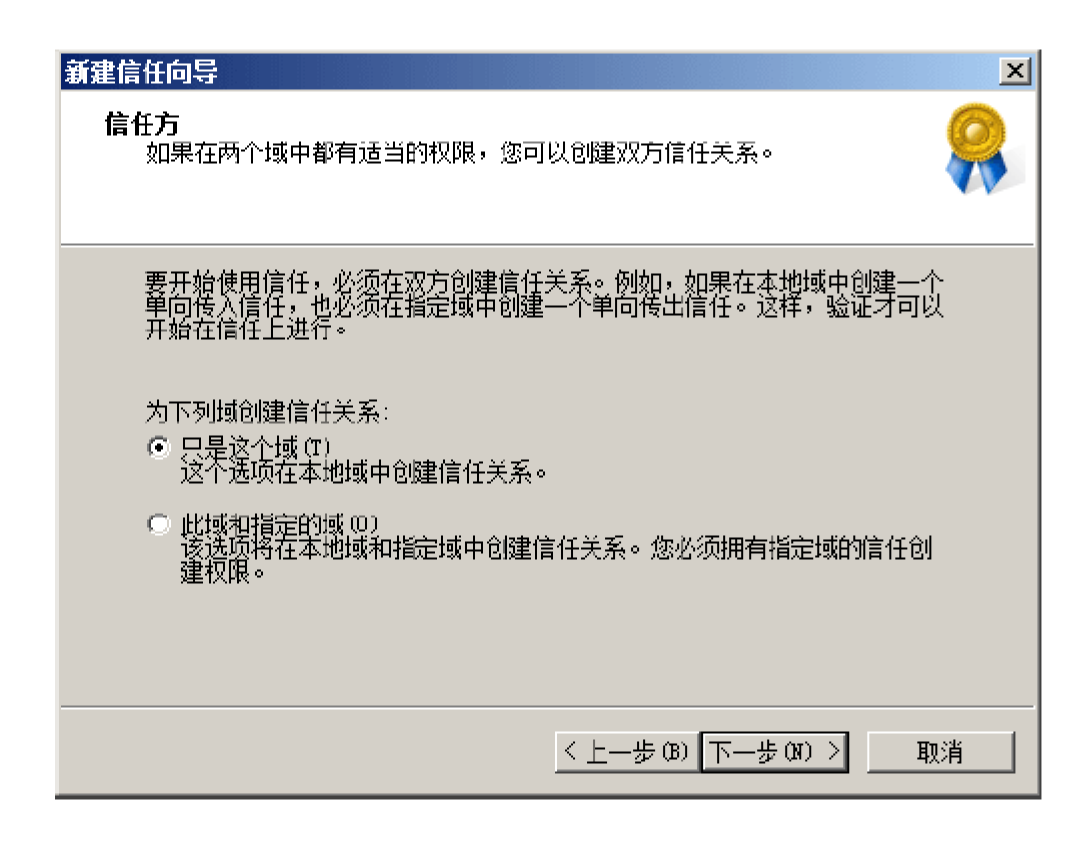


图 3-40　“信任方”界面

⑦　单击“下一步”按钮，显示如图 3-41 所示的“用户名和密码”界面，在“用户名”和“密码”文本框中，分别输入域控制器 hsnc.cn 上的管理员账户及密码。

⑧　单击“下一步”按钮，显示如图 3-42 所示的“选择信任完毕”界面，提示当前所作的信任关系设置。单击“上一步”按钮，可以返回，重新修改设置。

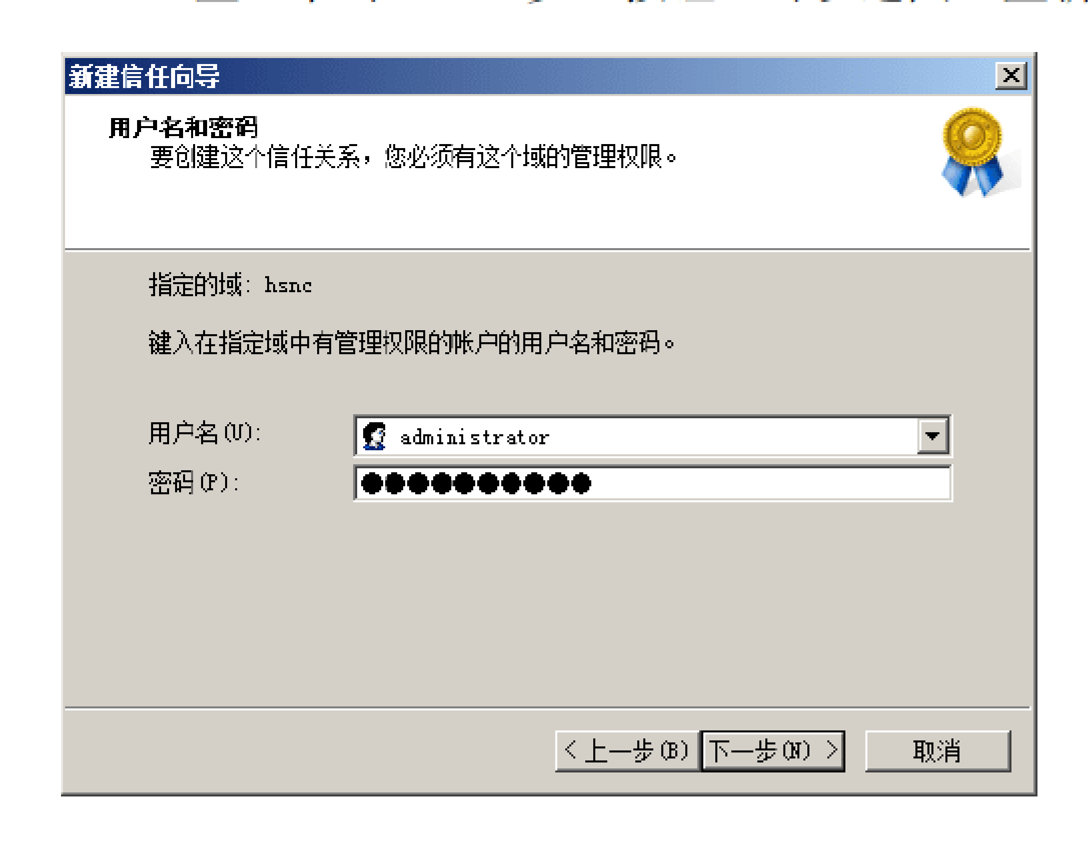


图 3-41　“用户名和密码”界面

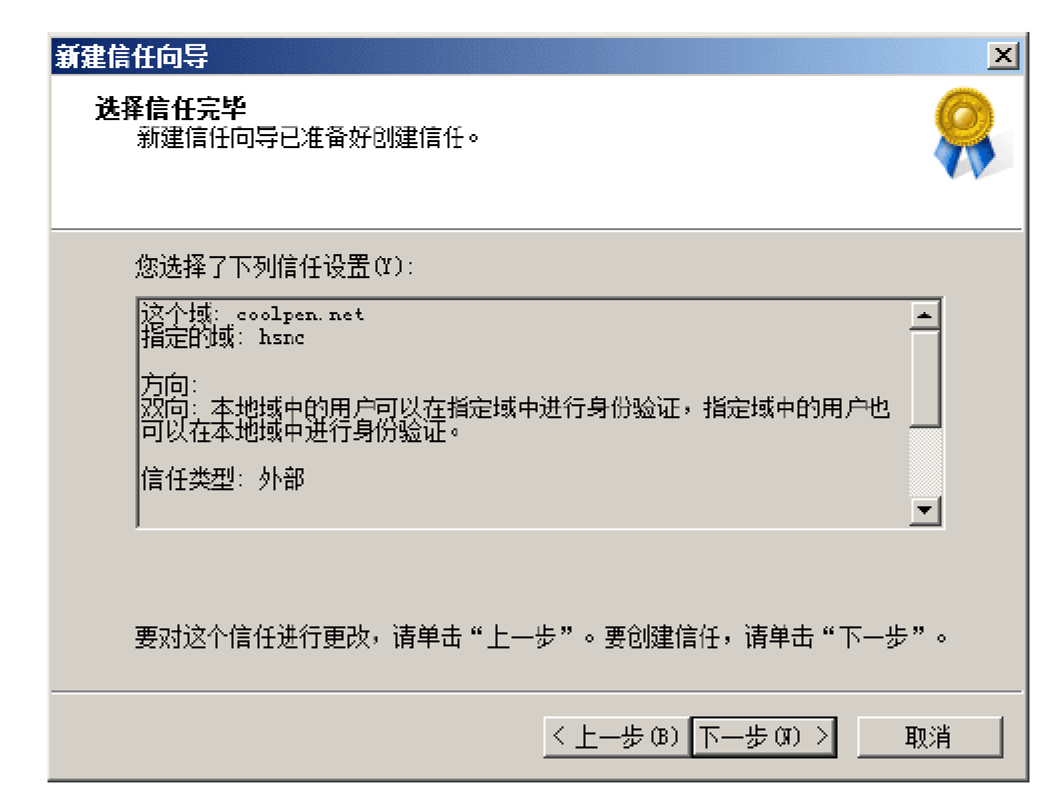


图 3-42　“选择信任完毕”界面

⑨　单击“下一步”按钮，开始创建信任关系，完毕后显示如图 3-43 所示的“信任创建完毕”界面。创建完毕后，还可继续对该信任关系的某些选项进行配置，根据创建过程中选择选项的不同，配置选项也会有所不同。

⑩　单击“下一步”按钮，显示如图 3-44 所示的“确认传出信任”界面，由于当前只是在其中一台域控制器上进行创建信任关系操作，只有在另一台域控制器上进行同样操作后方可完成信任关系的创建，所以此时无法进行信任传出验证，选择“否，不要确认传出信任”单选按钮即可。



图 3-43　“信任创建完毕”界面

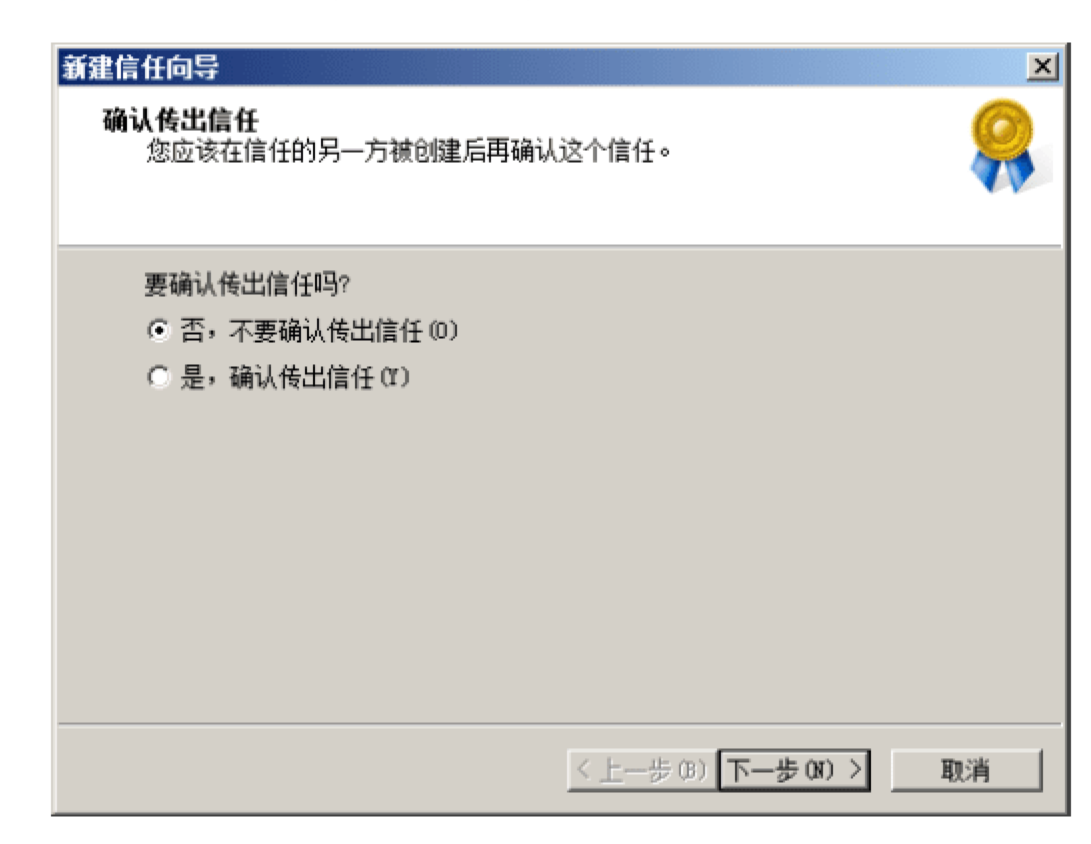


图 3-44　“确认传出信任”界面

⑪　单击“下一步”按钮，显示如图 3-45 所示的“确认传入信任”界面，同样选择“否，不确认传入信任”单选按钮即可。



提示：如果创建信任关系过程中选择的是“单向：传出”或者“单向：传入”信任方式，则配置过程中就不会同时出现“确认传入信任”和“确认传出信任”界面。

⑫ 单击“下一步”按钮，显示如图 3-46 所示的“正在完成新建信任向导”界面，提示创建信任关系成功。



图 3-45 “确认传入信任”界面

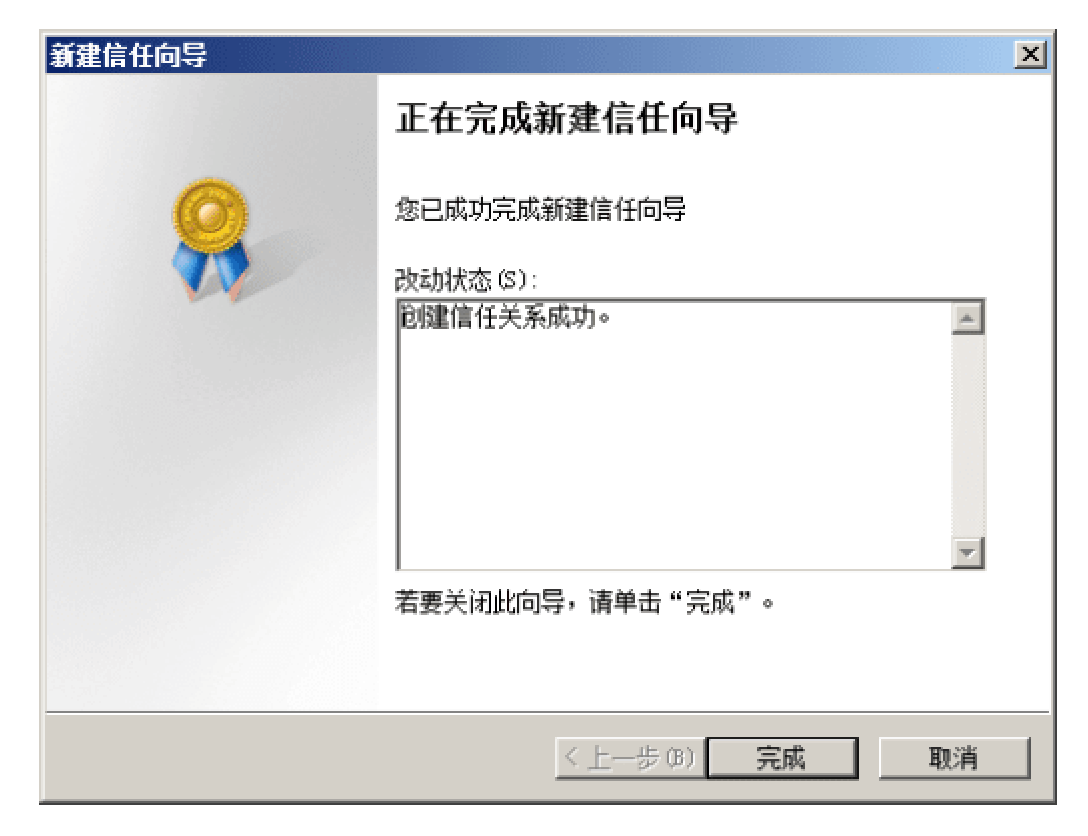


图 3-46 “正在完成新建信任向导”界面

⑬ 单击“完成”按钮关闭“新建信任向导”对话框，打开如图 3-47 所示的“Active Directory 域服务”对话框，提示已经启用 SID(安全识别符)筛选功能。SID 筛选用于防止可能试图将提升的用户权限授予其他用户账户的恶意用户攻击。强制 SID 筛选不会阻止同一林中的域迁移使用 SID 历史记录，而且也不会影响全局组的访问控制策略。对外部信任关系而言，SID 筛选功能会影响以下两个区域中的现有 Active Directory 基础结构：

- 将会从受信域发出的身份验证请求中删除 SID 历史数据，这些 SID 历史数据包含除该受信域外的所有域中的 SID。这会导致拒绝访问具有用户旧 SID 的资源。
- 林间通用组访问控制的策略将需要更改。

⑭ 单击“确定”按钮，返回“coolpen.net 属性”对话框，新创建的信任关系已经显示在列表中，如图 3-48 所示。

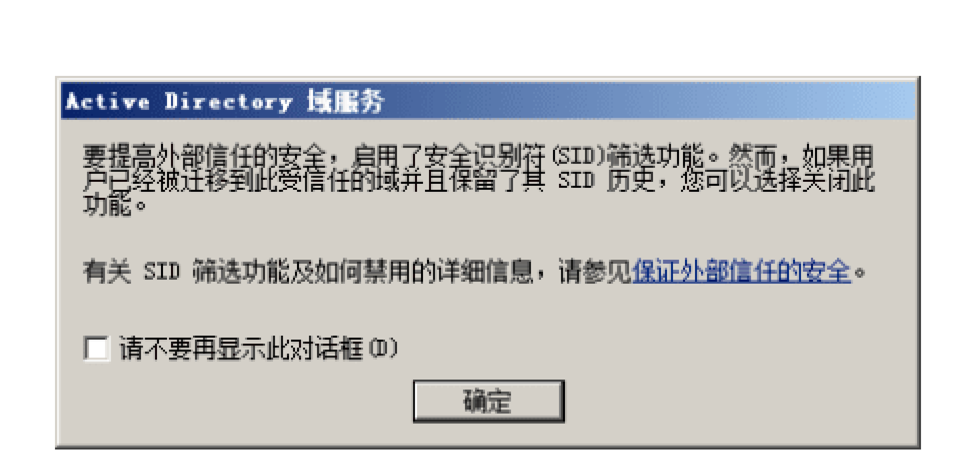


图 3-47 “Active Directory 域服务”对话框

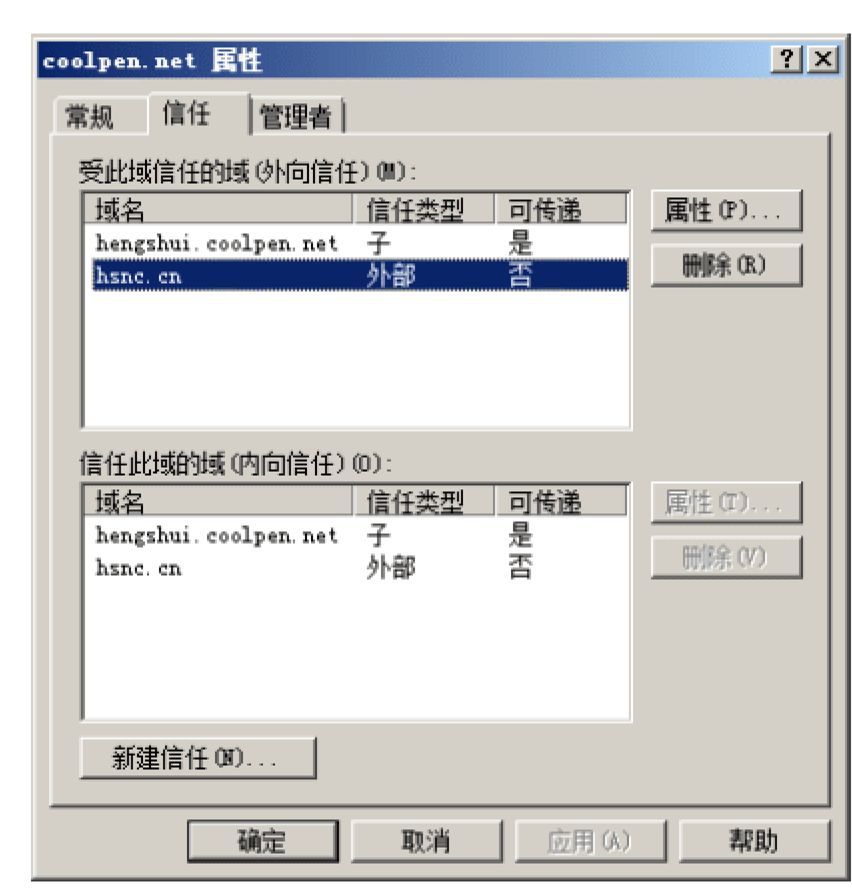


图 3-48 创建成功的信任关系

(2) 在另一台域控制器(本例中的 hsnc.cn)上，执行如下操作

① 打开“Active Directory 域和信任关系”窗口，右击域名 hsnc.cn，选择快捷菜单中的“属性”命令，打开“hsnc.cn 属性”对话框，切换至如图 3-49 所示的“信任”选项卡，默认已经显示了刚刚创建的信任关系。

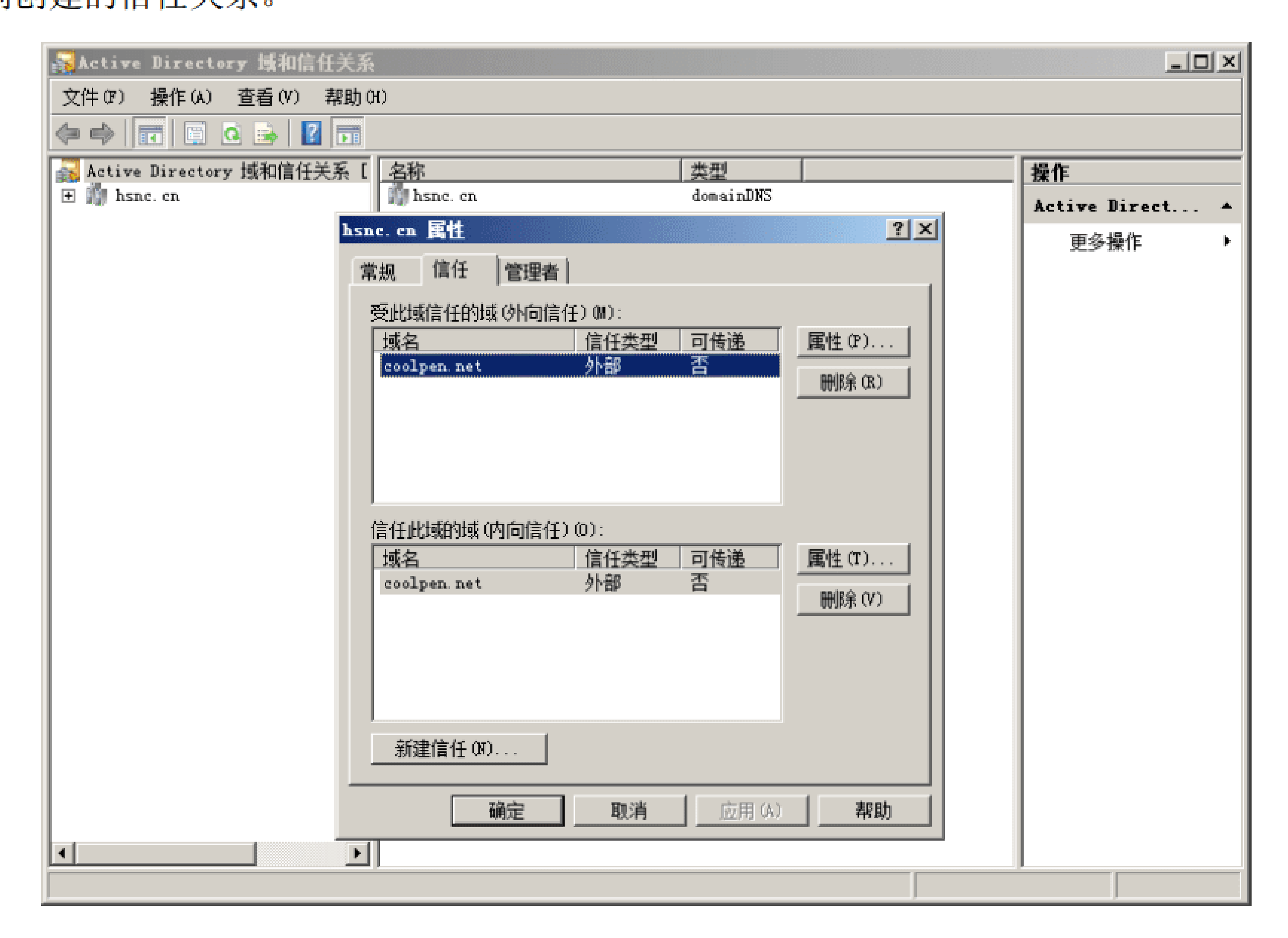
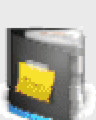


图 3-49　“hsnc.cn 属性”对话框



提示：如果创建的是单向信任关系，则已创建的信任关系只会出现在“受此域信任的域(外向信任)”或“此域信任的域(内向信任)”中的一个列表框中，但确认创建信任关系的操作步骤与双向信任完全相同。

② 在“受此域信任的域(外向信任)”列表框中，选择“coolpen.net”并单击其右侧的“属性”按钮，打开“coolpen.net 属性”对话框，如图 3-50 所示。

③ 单击“验证”按钮，显示如图 3-51 所示的“Active Directory 域服务”对话框，验证信任传入方向时，必须有对方域控制器的管理员权限。选择“是，验证传入信任”单选按钮，并在“用户名”下拉列表框和“密码”文本框中，分别输入域控制器 coolpen.net 上的管理员账户名称和密码。

④ 单击“确定”按钮，完成传入信任验证之后，还需要单击“信任此域的域(内向信任)”列表框右侧的“属性”按钮，执行同样操作，以完成传出信任的验证。

⑤ 域属性对话框的“身份验证”选项卡中，还可以对于用户在各个域上执行的身份验证方式进行选择，在如图 3-52 所示的“coolpen.net 属性”对话框中，可以为来自 coolpen.net 域的用户账户选择身份验证范围。

包括如下两种身份验证方式。

- 全域性身份验证：域控制器 coolpen.net 上的用户使用域控制器 hsnc.cn 上的资源时，需要通过两台域控制器上设置的所有身份验证方式。
- 选择性身份验证：域控制器 hsnc.cn 将不会对来自域控制器 coolpen.net 的用户访问进行任何身份验证，对 hsnc.cn 下属子域同样具有不受身份验证的“特权”。

至此，两台域控制器之间即可成功建立信任关系，这两个域的用户即可以自由访问另外一个域的信息

(如果选择单向信任则另当别论)。如图 3-53 所示，是一台加入域控制器 coolpen.net 主机名为 coolpen-c8 的计算机的登录窗口，在“登录到”下拉列表中显示了本地计算机、域控制器 coolpen.net 以及其所有信任的域，用户可根据需要选择登录到的对象。

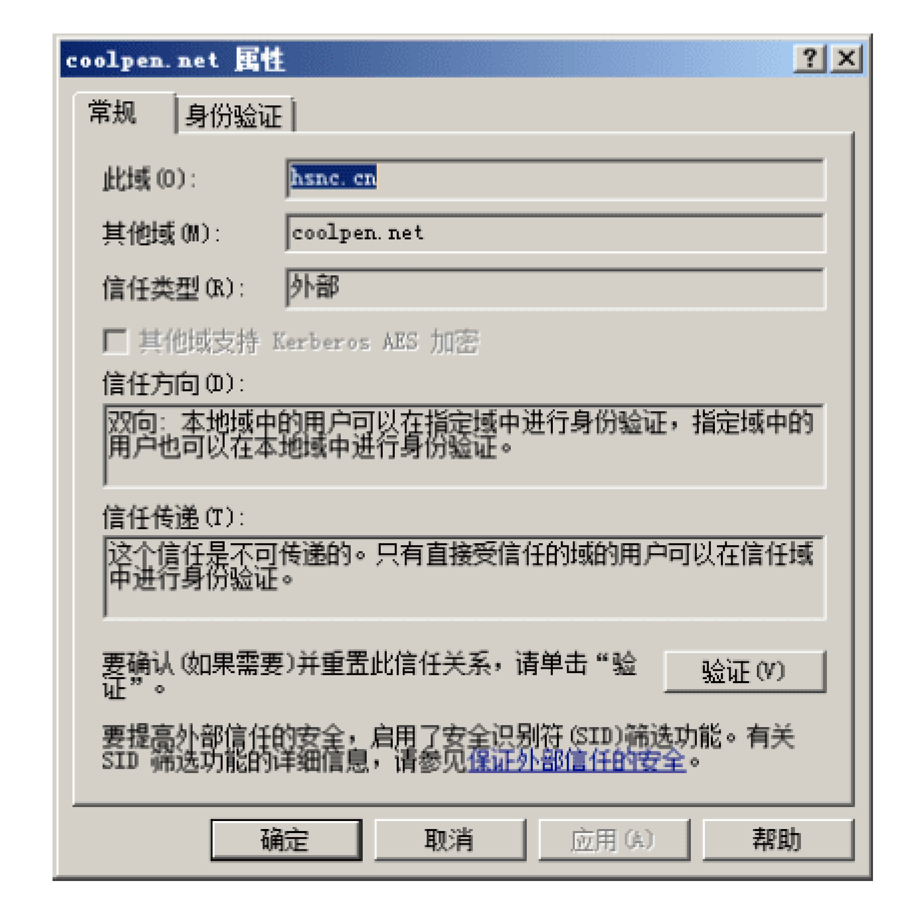


图 3-50 “coolpen.net 属性”对话框

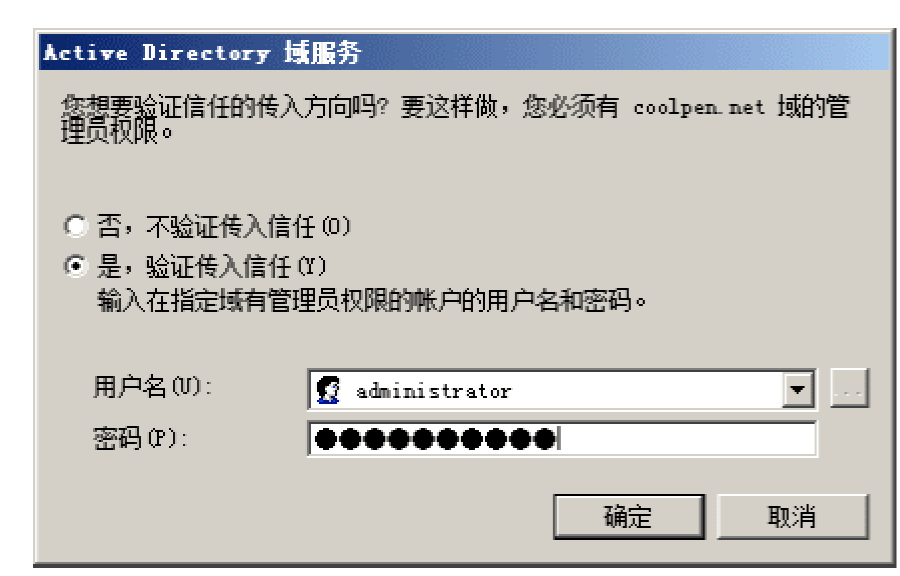


图 3-51 “Active Directory 域服务”对话框

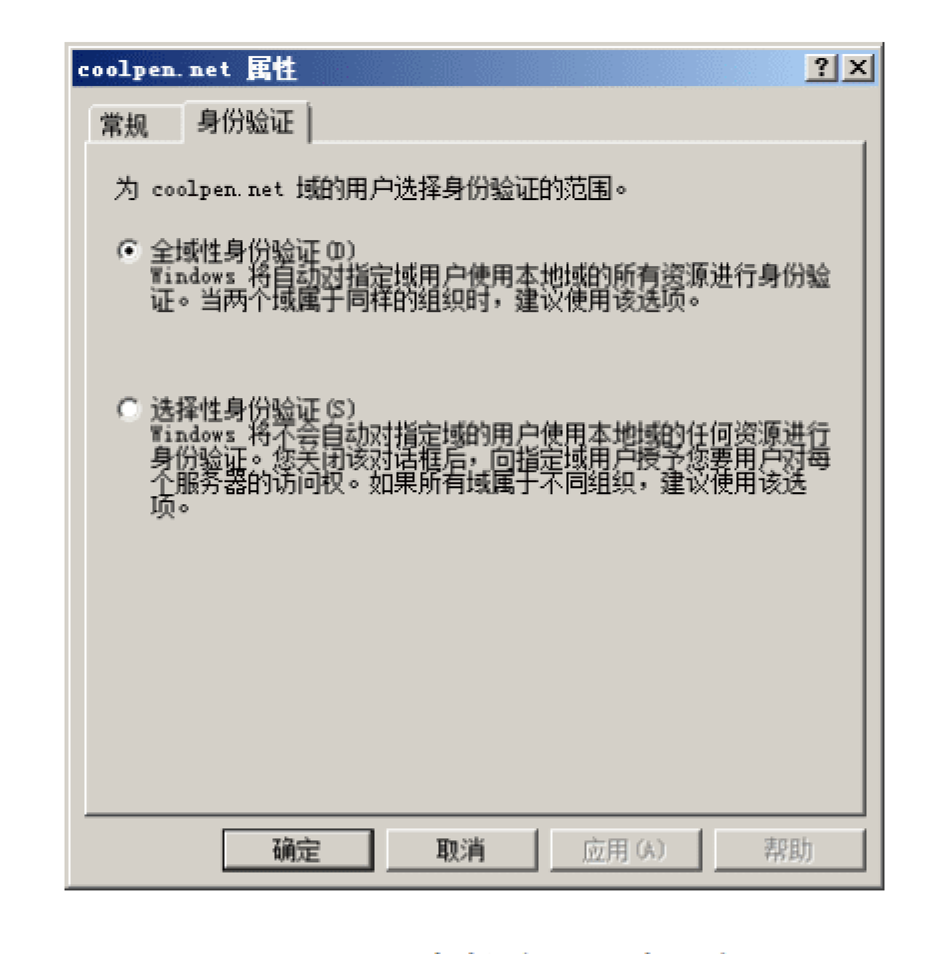


图 3-52 “身份验证”选项卡



图 3-53 “登录到 Windows”窗口

3.1.5 权限委派

委派是 Active Directory 最重要的安全功能之一，用于将某一功能的处理和管理的责任，分配给另一个用户、组或组织单位。通过委派管理，可以为适当的用户和组指派一定范围的管理任务，这样不仅可以减少需要具有较高管理权限的管理员用户账户数量，还可以为普通用户和组指派基本管理任务，而让 Domain Admins 和 Enterprise Admins 组的成员执行域范围和林范围的管理。通过委派管理，可以使组织内的组更多地控制他们的本地网络资源。还可以通过限制管理员组的成员，保护网络不受意外或恶意的损伤。通过委派，让信任用户可以在一个特定容器内改变属性、创建或删除某种类型的对象以及更改某种类型对象的

某些属性等。

1. 权限委派概述

通过在域中创建组织单位，并将特定组织单位的管理控制权委派给特定用户或组，可将管理控制权委派给域树的任何层次。通常情况下，可以向以下 Active Directory 容器委派管理权限：

- 组织单位。
- 域。
- 站点。

(1) 域和组织单位委派

在 Windows Server 2003 操作系统中，管理员可以通过创建多个组织单位，并将适当的管理权限委派到其中的对象上。要委派管理权限，可以修改容器的任意访问控制列表(DACL)，将对域或组织单位的特定权限授予一个组。默认情况下，域管理员(Domain Admins)安全组的成员拥有对整个域委派控制权限。可以委派的日常任务包括：

- 将计算机加入域。
- 管理组策略链接。
- 创建、删除和管理用户账户。
- 重设用户账户的密码。
- 读取所有用户信息。
- 创建、删除和管理组。
- 修改一个组的成员。
- 管理打印机。
- 创建和删除打印机。
- 管理组策略链接。

因为组织单位用于管理委派，但自身并不是安全主管，所以由用户对象的父 OU 说明该用户对象的管理者。但并未说明这个特定用户可以访问哪些资源。

(2) 站点委派

使用“Active Directory 站点和服务”委派对站点、容器、站点间传输(IP 或 SMTP)或子网的控制权，这些实体的委派控制使受委派的管理员能够管理这些实体，但并未赋予管理员管理该实体内用户或计算机的能力。

例如，当委派对一个站点的控制权时，既可以委派对所有对象的控制权，也可以委派对该站点上的一个或多个对象的控制权。可以委派控制权的对象包括用户对象、计算机对象、组对象、打印机对象、部门对象、共享文件夹对象、站点对象、站点链接对象、站点链接桥对象等。然后，就会提示选择要委派权限的范围(常规、属性特有的或仅仅是特定子对象的创建或删除)。如果指定的是常规范围，则会提示授予以下一个或多个权限：完全控制、读取、写入、创建所有子对象、删除所有子对象、读取所有属性或写入所有属性。

2. 权限委派

管理员可以通过如下两种方式实现权限委派。

(1) 安全组权限委派

在 Windows Server 2003 或 Windows Server 2008 域控制器安装过程中，默认已经创建了多个安全组，如 Administrators、Domain Admins 等，这些组中的成员通常拥有执行整个域或本地域控器上某些安全操作的权限。系统默认安全组的成员，通常情况下不宜轻易更改，以免影响系统安全。如遇特殊情况需要增加安全管理员数量时，可以自定义新的安全组，并将安全控制权限委派给该组，主要操作步骤如下。

① 依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开 “Active Directory 用户和计算机”窗口，选择目标组织单位，并新建一个安全组，如图 3-54 所示。在“组作用域”选项区域中，选择“全局”单选按钮，在“组类型”选项区域中选择“安全组”单选按钮。

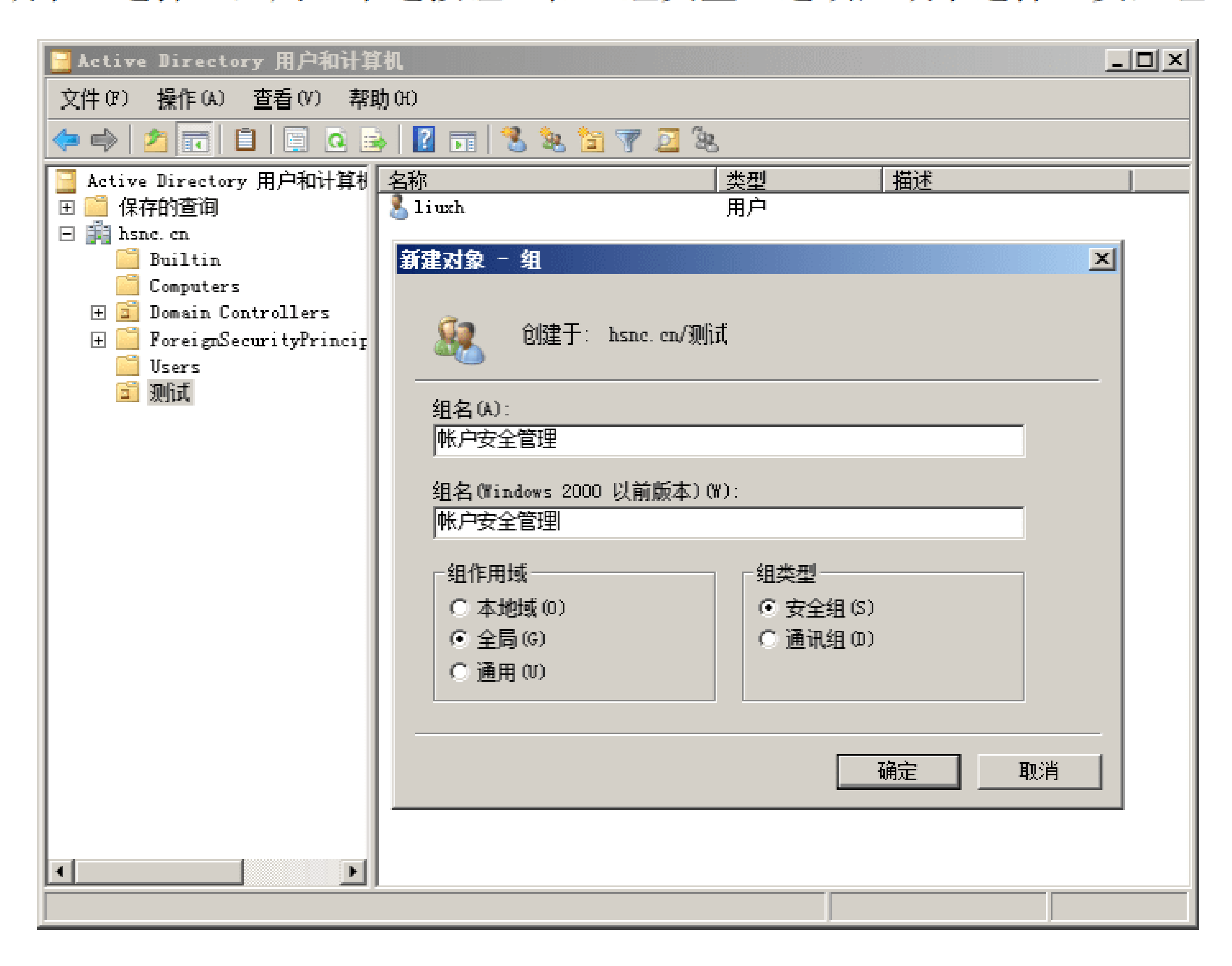


图 3-54 新建安全组

② 单击“确定”按钮，完成安全组的创建。右击该安全组并选择快捷菜单中的“属性”命令，打开安全组属性对话框，切换至如图 3-55 所示的“安全”选项卡。



图 3-55 “账户安全管理 属性”对话框



提示：如果打开的组属性对话框中，没有“安全”选项卡，可以在“Active Directory 用户和计算机”窗口中，依次选择“查看”→“高级功能”命令使其显示，如图 3-56 所示。

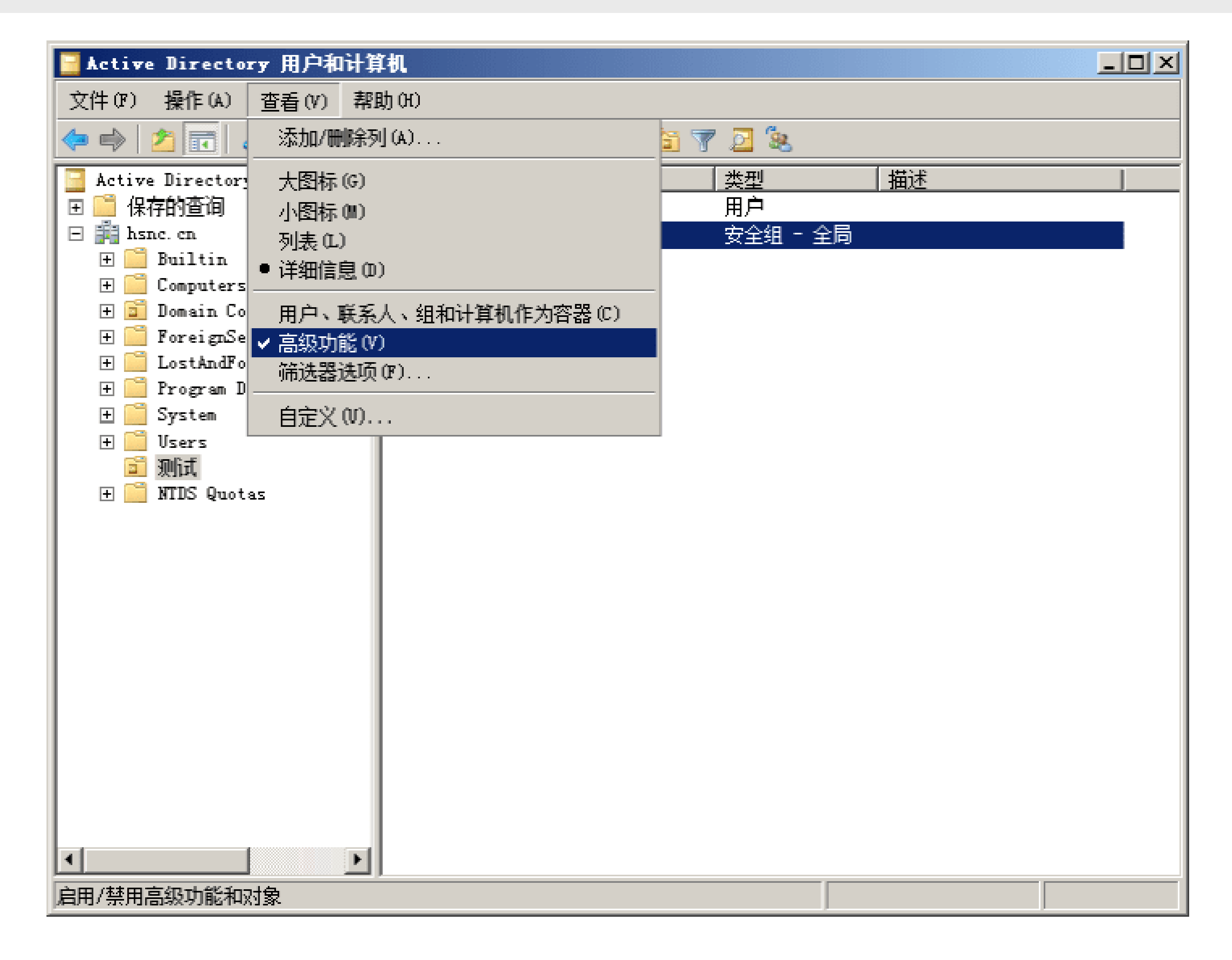
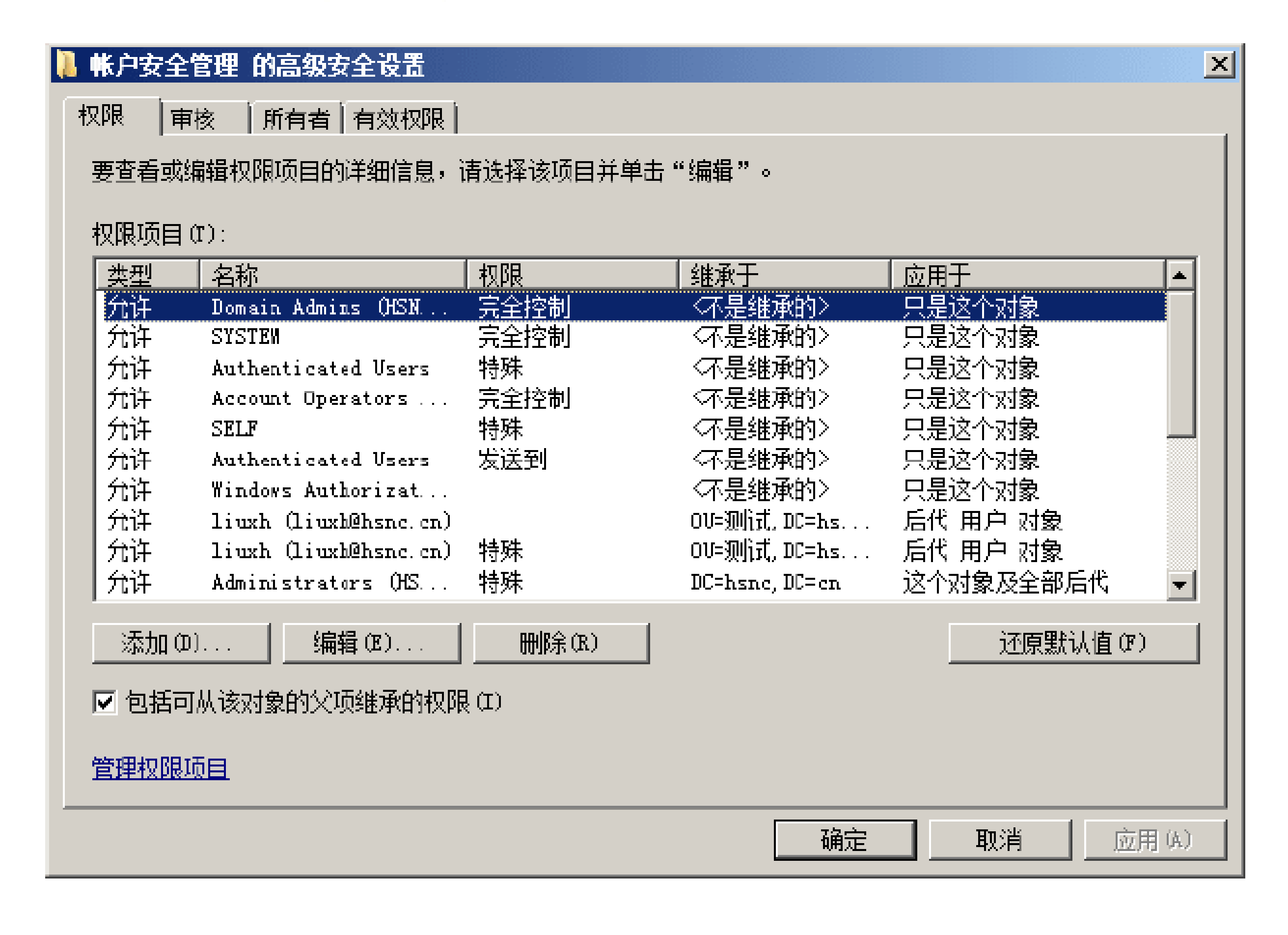


图 3-56 使用高级功能

③ 单击“高级”按钮，显示如图 3-57 所示的“账户安全管理 的高级安全设置”对话框，可以查看可用于该对象的所有权限项目。

④ 单击“添加”按钮，显示如图 3-58 所示的“选择用户、计算机或组”对话框，输入想要添加的组、计算机或用户的名称。



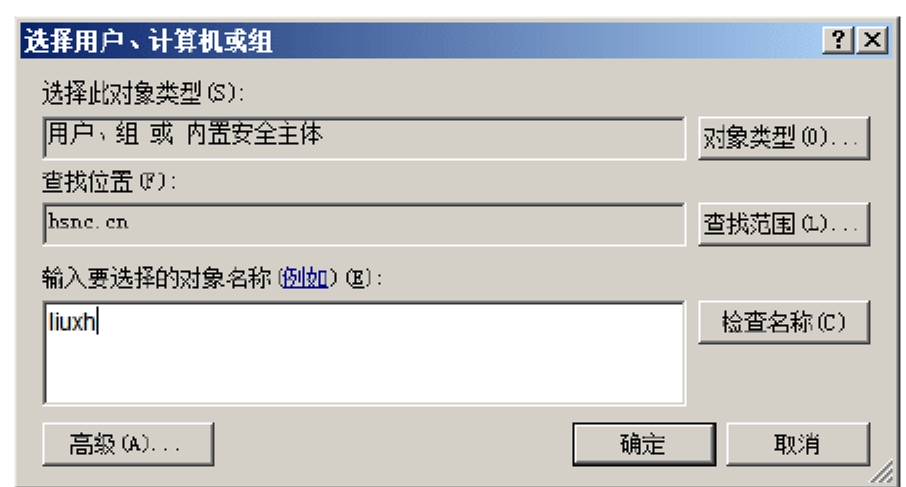


图 3-57 “账户安全管理 的高级安全设置”对话框

图 3-58 “选择用户、计算机或组”对话框

⑤ 单击“确定”按钮，显示如图 3-59 所示的“账户安全管理 的权限项目”对话框。此处需要委派的是针对用户账户安全管理的权限，如更改密码、重设密码等，所以需要在“应用于”下拉列表框中选择“后代 用户 对象”，并在“权限”列表框中，选中“更改密码”和“重置密码”复选框。

⑥ 单击“确定”按钮，即可完成赋予用户对其后代账户的安全密码管理权限。如果需要设置其他的权限，根据需要设置相关的权限即可。切记，不要轻易赋予用户“完全控制”的权限！

(2) 用户权限委派向导

权限委派向导是比较常用的权限委派方法之一。例如，同样将重置密码权限委派给 liuxh 用户账户，可以按照如下步骤操作。

① 打开“Active Directory 用户和计算机”窗口，右击需要委派管理权限对象所在的 OU(如“测试”)，选择快捷菜单中的“委派控制”命令，显示如图 3-60 所示的“控制委派向导”对话框。

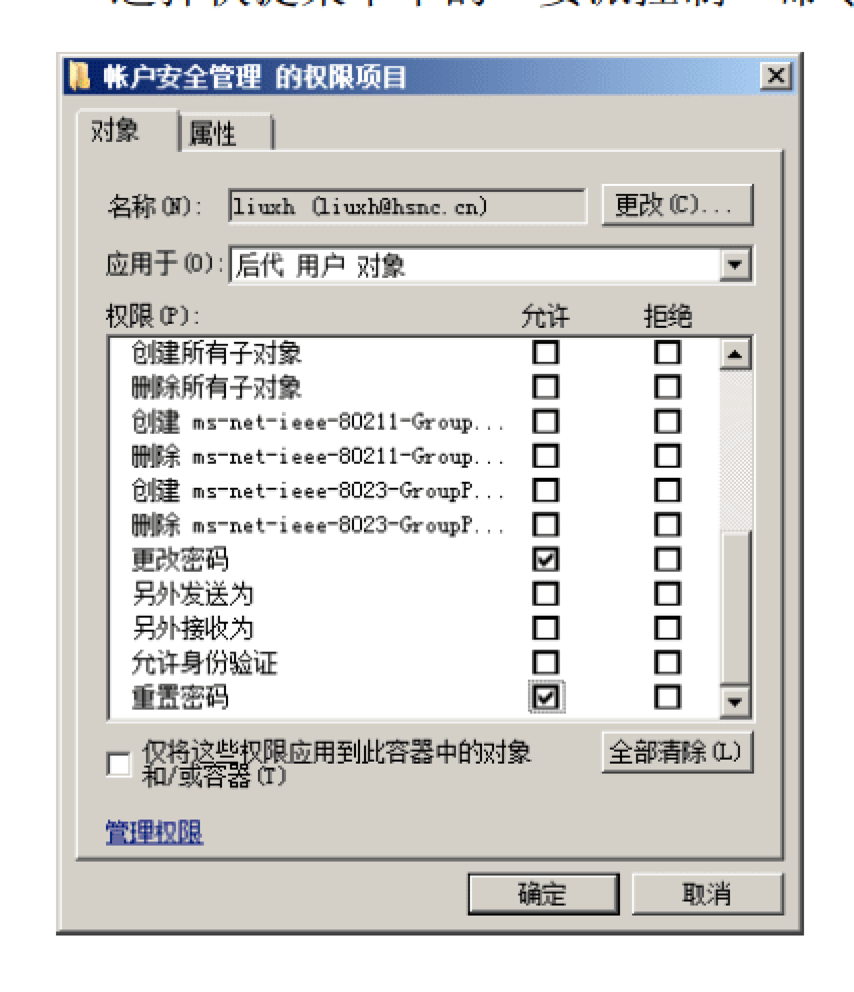
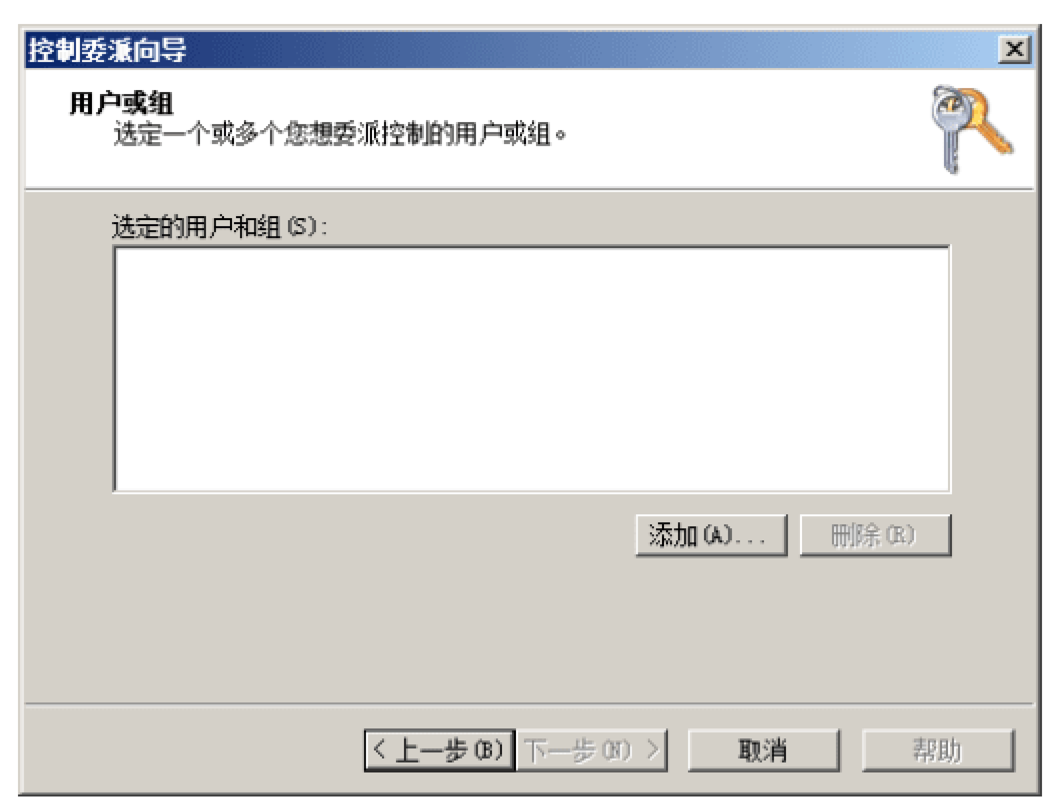


图 3-59 “账户安全管理 的权限项目”对话框

图 3-60 “控制委派向导”对话框

② 单击“下一步”按钮，显示如图 3-61 所示的“用户或组”界面。

③ 单击“添加”按钮，显示如图 3-62 所示的“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中输入接受权限的用户账户名称，如“liuxh”，单击“确定”按钮，将其添加到“选定的用户和组”列表框中。





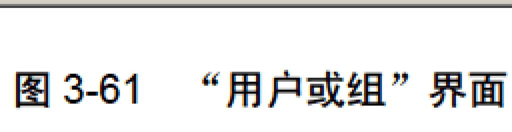


图 3-61 “用户或组”界面

图 3-62 “选择用户、计算机或组”对话框

④ 单击“下一步”按钮，显示如图 3-63 所示的“要委派的任务”界面。在“委派下列常见任务”列表框中，选中“重置用户密码并强制在下次登录时更改密码”复选框。

⑤ 单击“下一步”按钮，显示如图 3-64 所示的“完成控制委派向导”界面，提示前面所设置的委派权限信息。

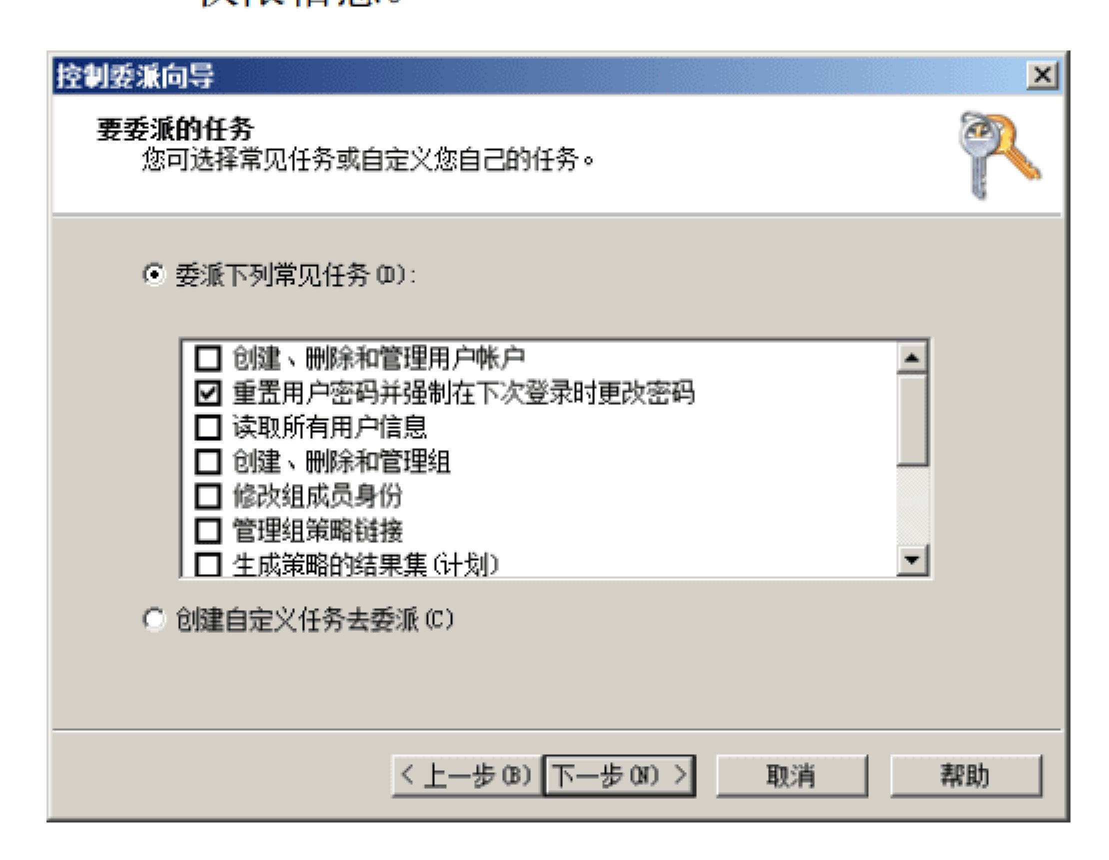


图 3-63 “要委派的任务”界面



图 3-64 “完成控制委派向导”界面

⑥ 单击“完成”按钮，即可完成委派任务操作。

3.1.6 只读域控制器

只读域控制器(RODC)是在 Windows Server 2008 操作系统中一种新的域控制器。使用只读域控制器，可以很容易地在物理安全得不到保证的地区部署域控制器，在只读域控制器中包含活动目录数据库的只读部分。

1. 只读 ADDS 数据库

除账户密码之外，RODC 保存了可写域控制器上所保留的所有 Active Directory 对象和属性，但对存储在 RODC 上的数据库只有读权限，不能进行任何更改。如果想要更改这些数据，则必须在可写域控制器上进行，然后再复制回 RODC。

请求对目录的读取访问的本地应用程序可以获取访问权限。请求写入访问的轻型目录应用程序协议(LDAP)应用程序将接收 LDAP 引用响应，此响应会被定向到可写域控制器。

2. 单向复制

可读写域控制器之间的复制是双向的，而 RODC 和可读写域控制器之间的复制是单向的，RODC 通过分布式文件系统(DFS)从可读写域控制器复制数据。此时，恶意用户在分支位置进行的任何更改或损坏，都不能从 RODC 复制到林的其余部分。

3. 密码缓存

默认情况下，RODC 上只存储本地的计算机账户和一个用于 RODC 特殊的 Kerberos 票据授权(KRBTGT)账户，此账户被可读写域控制器用来验证 RODC 身份。在可读写域控制器上启用密码缓存功能，即可在 RODC 上缓存所有域用户账户。如果在 RODC 上启用密码缓存，只会影响缓存到本地计算机的用户账户。

在账户成功经过身份验证后，RODC 将尝试与中心站点中的可写域控制器联系并请求获取相应凭据的副本。可写域控制器可以识别出请求来自某个 RODC，并查询对该 RODC 有效的密码复制策略。

密码复制策略确定是否可以将用户凭据或计算机凭据从可写域控制器复制到 RODC。如果密码复制策略允许复制凭据，则可写域控制器将凭据复制到 RODC，然后 RODC 缓存凭据。

在 RODC 上缓存凭据后，RODC 即可直接验证用户的登录请求，直到对凭据进行更改。通过将凭据缓存，只能通过 RODC 验证身份的用户，使危害 RODC 而使凭据泄露的可能性也得到限制。通常情况下，在任何给定的 RODC 上只缓存一小部分域用户的凭据。因此，如果出现 RODC 被窃的情况，只有 RODC 上缓存的那些凭据可能会被破解。

保持凭据缓存处于禁用状态可能进一步限制泄露，但同时也可能使所有身份验证请求被转发到可写域控制器。管理员可以通过修改默认密码复制策略，允许在 RODC 上缓存用户凭据。具体密码复制策略可以在域控制器的属性对话框中进行设置，如图 3-65 所示。

4. 只读 DNS

在实际使用中，建议在 RODC 上安装 DNS 服务，RODC 可以复制 DNS 使用的所有应用程序目录分区中的数据，包括 ForestDNSZones 和 DomainDNSZones，支持客户端请求 RODC 进行名称解析。如果已在 RODC 上安装了 DNS 服务器，则客户端可以与查询任何其他 DNS 服务器一样，查询该 DNS 服务器以进行名称解析。

但是，RODC 上的 DNS 服务器不直接支持客户端更新。因此，RODC 不为其承载的任何 Active Directory 集成区域注册名称服务器(NS)资源记录。当客户端尝试根据 RODC 更新其 DNS 记录时，服务器会返回一个引用。然后客户端可以尝试对引用中提供的 DNS 服务器进行更新。在后台，RODC 上的 DNS 服务器尝试从进行更新的 DNS 服务器复制更新记录。

5. RODC 管理

在可读写的域控制器中，本地管理员和域管理员都可以管理域控制器。而对于 RODC，则允许一个普通的域用户成为 RODC 的本地管理员，设置的域用户可以在 RODC 所在的区域执行管理任务，此用户在域中或者任何可读写的域控制器上没有用户权利，仅管理区域分支机构的权限，所以不会影响 Active Directory 的整体安全性。

6. RODC 部署要求

如果需要部署 RODC，在网络中必须有一台安装或者升级到 Windows Server 2008 的域控制器。部署之前，管理员应注意以下事项：

- Active Directory 数据库复制。RODC 支持从 Windows Sever 2003 域控制器复制架构分区和配置分区的数据，但是 RODC 只能从来自同一域的 Windows Server 2008 的可读写域控制器复制域分区的数据更新。因此，在网络中至少安装一台 Windows Server 2008 的域控制器用于 RODC 复制。
- 林功能级别。部署 RODC 需要森林的功能级别最低为 Windows Server 2003 模式，建议使用 Windows Server 2008 模式。用户可以通过“Active Directory 域和信任关系”窗口提升到所需的林功能级别。
- Windows Server 2008 域控制器的角色为主域控制器，否则将无法识别 RODC 使用的特殊 Kerberos 票据授权票(KRBTGT)账户。
- RODC 默认不缓存账户，必须在可读写域控制器上启用账户缓存功能后，才可以用于缓存域用户账户。
- RODC 安装完成后，默认连接的是当前所有的可读写域控制器，必须在 RODC 上通过“更改域控

制器”使其连接到已部署的 RODC 上。

7. 安装 RODC

① 选择“开始”→“运行”命令，打开“运行”对话框，在“打开”文本框中，输入“Dcpromo.exe”，单击“确定”按钮。显示如图 3-66 所示的“Active Directory 域服务安装向导”对话框，选中“使用高级模式安装”复选框。





图 3-65　属性对话框　　　　图 3-66　“Active Directory 域服务安装向导”对话框

② 单击两次“下一步”按钮，显示如图 3-67 所示的“选择某一部署配置”界面。选择“现有林”单选按钮，然后选择“向现有域添加域控制器”单选按钮。

③ 单击“下一步”按钮，显示如图 3-68 所示的“网络凭据”界面。因为这里本地计算机已经加入到域中，并且登录的账户是管理员账户，所以选择“我的当前登录凭据(域\用户名)”单选按钮即可。如果当前计算机还未加入到域中，可以选择“备用凭据”单选按钮，并单击“设置”按钮，设置所要使用的账户。



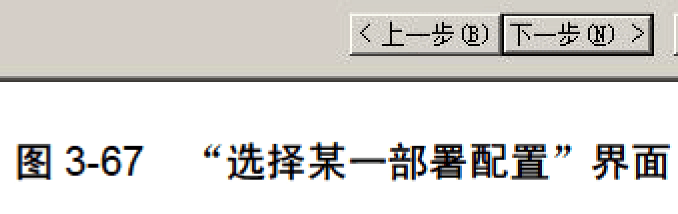




图 3-67　“选择某一部署配置”界面　　　　图 3-68　“网络凭据”界面

④ 单击“下一步”按钮，显示如图 3-69 所示的“选择一个域”界面。安装向导自动查找 coolpen.net 域的林根域。

⑤ 单击“下一步”按钮，显示如图 3-70 所示的“请选择一个站点”界面，保持默认值即可。



图 3-69 “选择一个域”界面



图 3-70 “请选择一个站点”界面

⑥ 单击“下一步”按钮，显示如图 3-71 所示的“其他域控制器选项”界面，选中“DNS 服务器”和“只读域控制器(RODC)”复选框。

⑦ 单击“下一步”按钮，显示如图 3-72 所示的“指定密码复制策略”界面。在该界面中，设置允许域控制器缓存到 RODC 域控制器中的账户。密码复制策略决定了用户或者计算机的凭据是否可以从可写域控制器复制到 RODC。如果策略允许，可写域控制器将密码复制到 RODC 上，并且 RODC 缓存用户或者计算机凭据。单击“添加”按钮，即可设置可以缓存到 RODC 域控制器中的用户、组和计算机。



图 3-71 “其他域控制器选项”界面

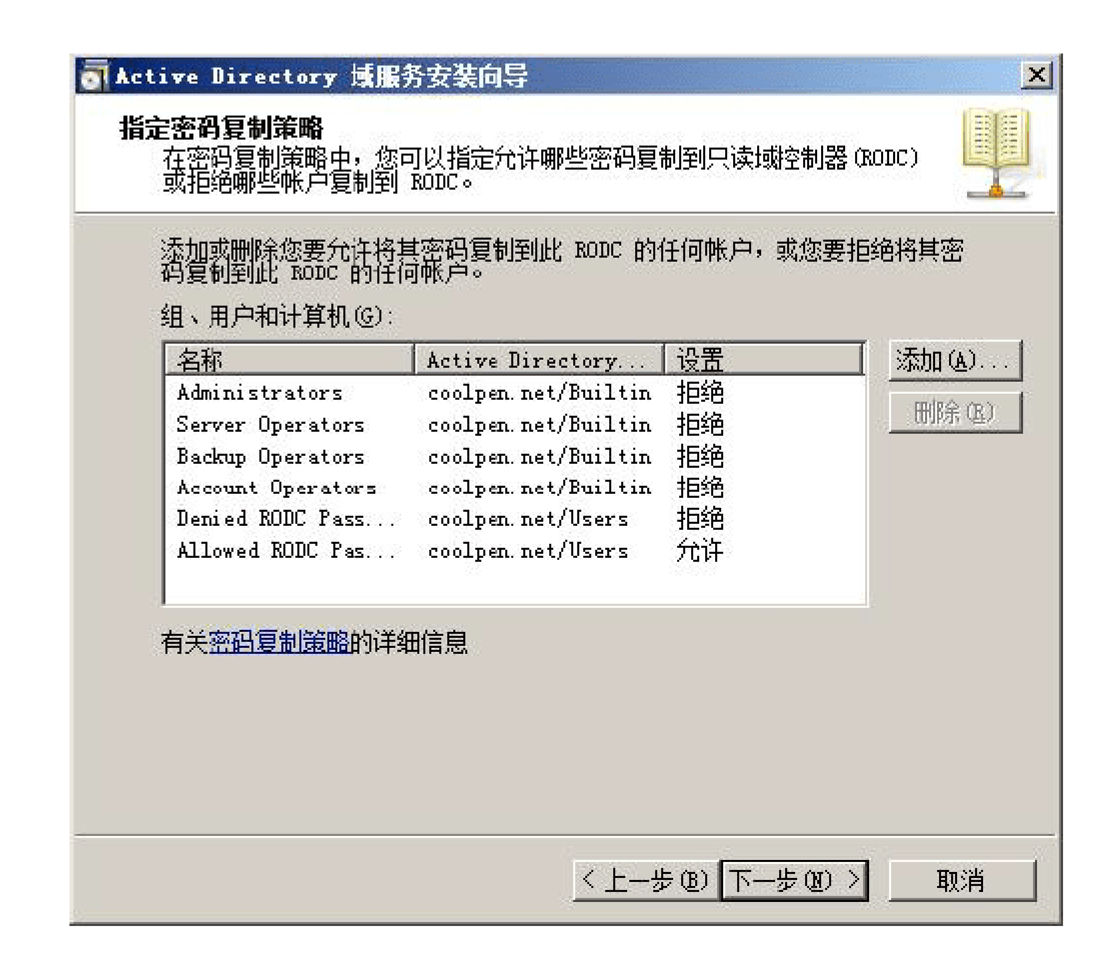


图 3-72 “指定密码复制策略”界面

⑧ 单击“下一步”按钮，显示如图 3-73 所示的“用于 RODC 安装和管理的委派”界面。设置管理 RODC 域控制器的管理账户。如果多人具备对 RODC 域控制器的管理权限，建议创建用户组，赋

予用户组管理 RODC 域控制器的权限。

⑨ 单击“下一步”按钮，显示如图 3-74 所示的“从介质安装”界面。设置缓存账户的方法，提供两种缓存类型，即通过域控制器复制数据和通过介质(共享或者光盘)复制。具体使用方法可根据实际需要进行选择，这里选择“通过网络从域控制器复制数据”单选按钮。

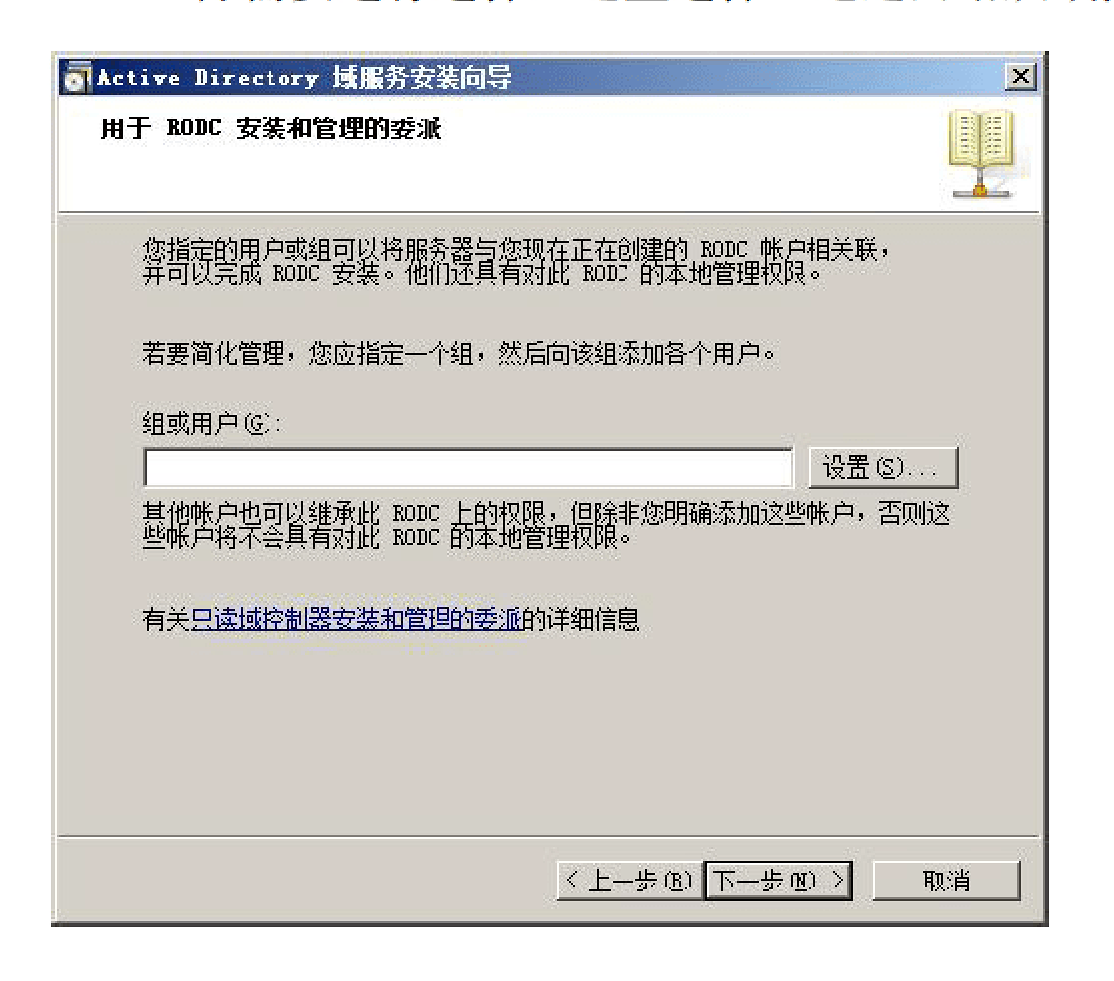


图 3-73　“用于 RODC 安装和管理的委派”界面

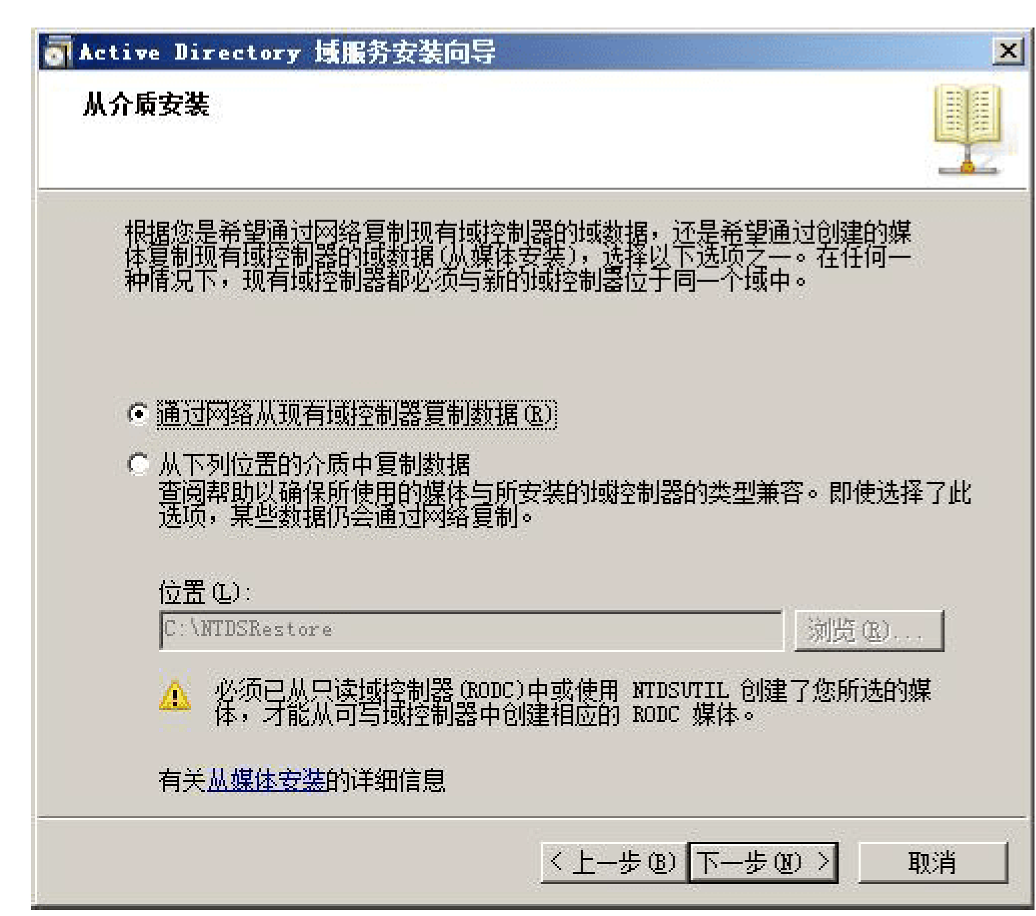


图 3-74　“从介质安装”界面

⑩ 单击“下一步”按钮，显示如图 3-75 所示的“源域控制器”界面。设置缓存账户的源域控制器，通常情况下源域控制器是域中的第一台域控制器。在“域控制器名称”列表中，选择源域控制器即可。

⑪ 单击“下一步”按钮，显示如图 3-76 所示的“数据库、日志文件和 SYSVOL 的位置”界面。建议将数据库、日志文件和 SYSVOL 文件夹分开存储在不同的物理磁盘中。

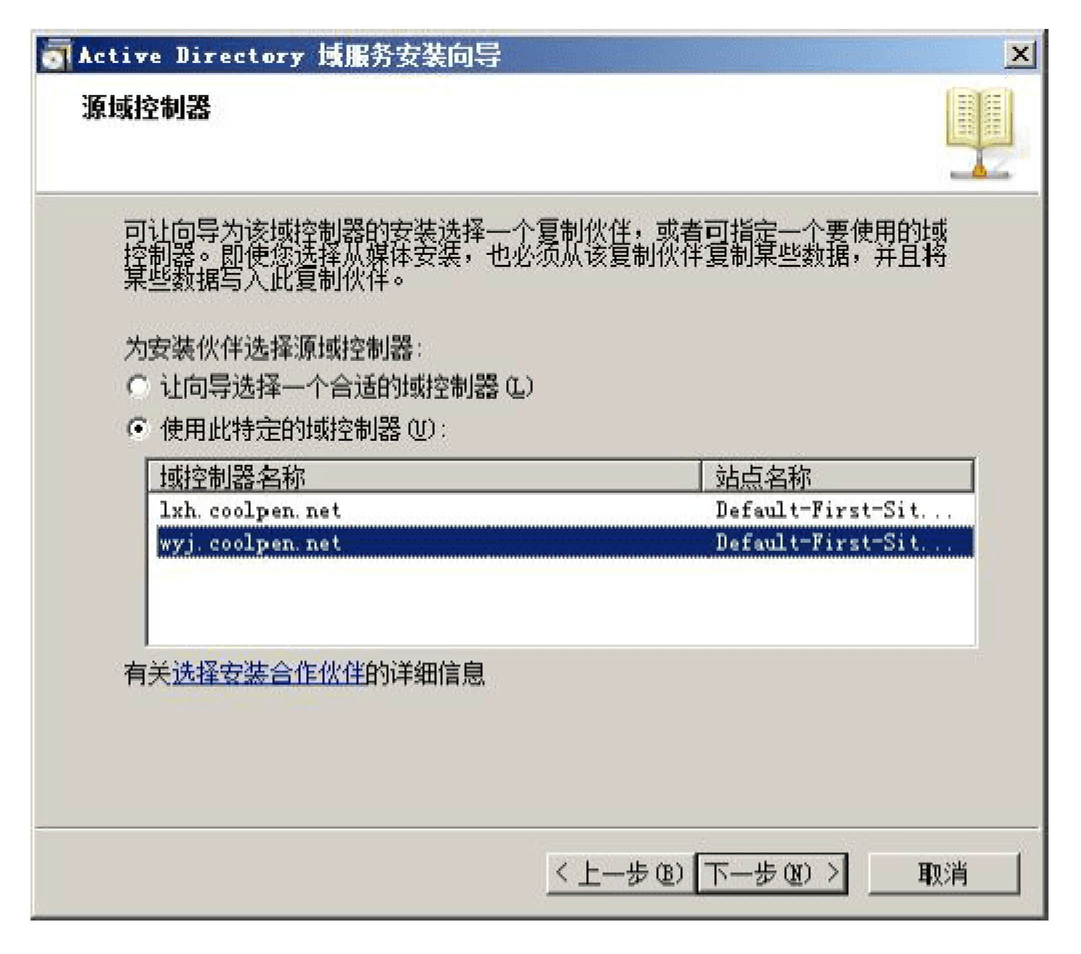


图 3-75　“源域控制器”界面

图 3-76　“数据库、日志文件和 SYSVOL 的位置”界面

⑫ 单击“下一步”按钮，显示如图 3-77 所示的“目录服务还原模式的 Administrator 密码”界面。需要注意的是，目录服务还原密码需要使用符合强密码策略标准的密码。

⑬ 单击“下一步”按钮，显示如图 3-78 所示的“摘要”界面，显示 RODC 配置信息。



图 3-77 “目录服务还原模式的 Administrator 密码”界面



图 3-78 “摘要”界面

⑭ 单击“下一步”按钮，开始安装 RODC 域控制器。安装完成后，显示如图 3-79 所示的“完成 Active Directory 域服务安装向导”界面。

⑮ 单击“完成”按钮，关闭安装向导，显示如图 3-80 所示的“Active Directory 域服务安装向导”提示对话框，提示管理员需要重新启动计算机。

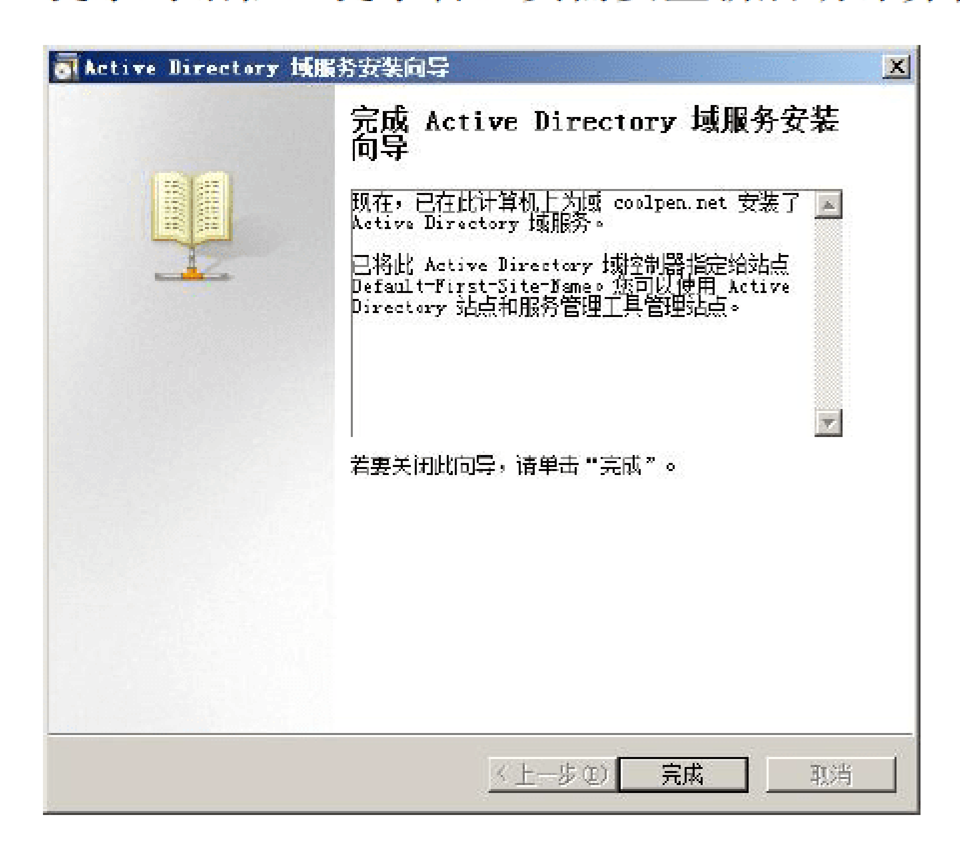


图 3-79 “完成 Active Directory 域服务安装向导”界面

Active Directory 域服务安装向导
必须重新启动计算机，Active Directory 域服务安装向导所做的更改才能生效。
立即重新启动(R)　不立即重新启动(D)

图 3-80 提示管理员需要重新启动计算机

⑯ 单击“立即重新启动”按钮，重新启动计算机，RODC 域控制器安装成功。

8. 添加缓存账户

在主域控制器中，设置可以在 RODC 上缓存的用户分支机构。建议为分支机构创建单独的组织单位，在该组织单位下创建组，组的创建规则建议符合企业的行政管理架构，以降低管理的复杂度。默认情况下，RODC 并未保存所有域用户账户的信息，可以按照如下方法，将需要缓存的用户账户添加到 RODC 的缓存策略中。

① 在 RODC 上，依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，打开如图 3-81 所示的“Active Directory 用户和计算机”窗口。依次选择 coolpen.net→Domain Controllers，此时，即可查看当前登录的域控制器的状态为“只读”。

② 双击“HSLXH”显示“HSLXH 属性”对话框，切换到如图 3-82 所示的“密码复制策略”选项卡。

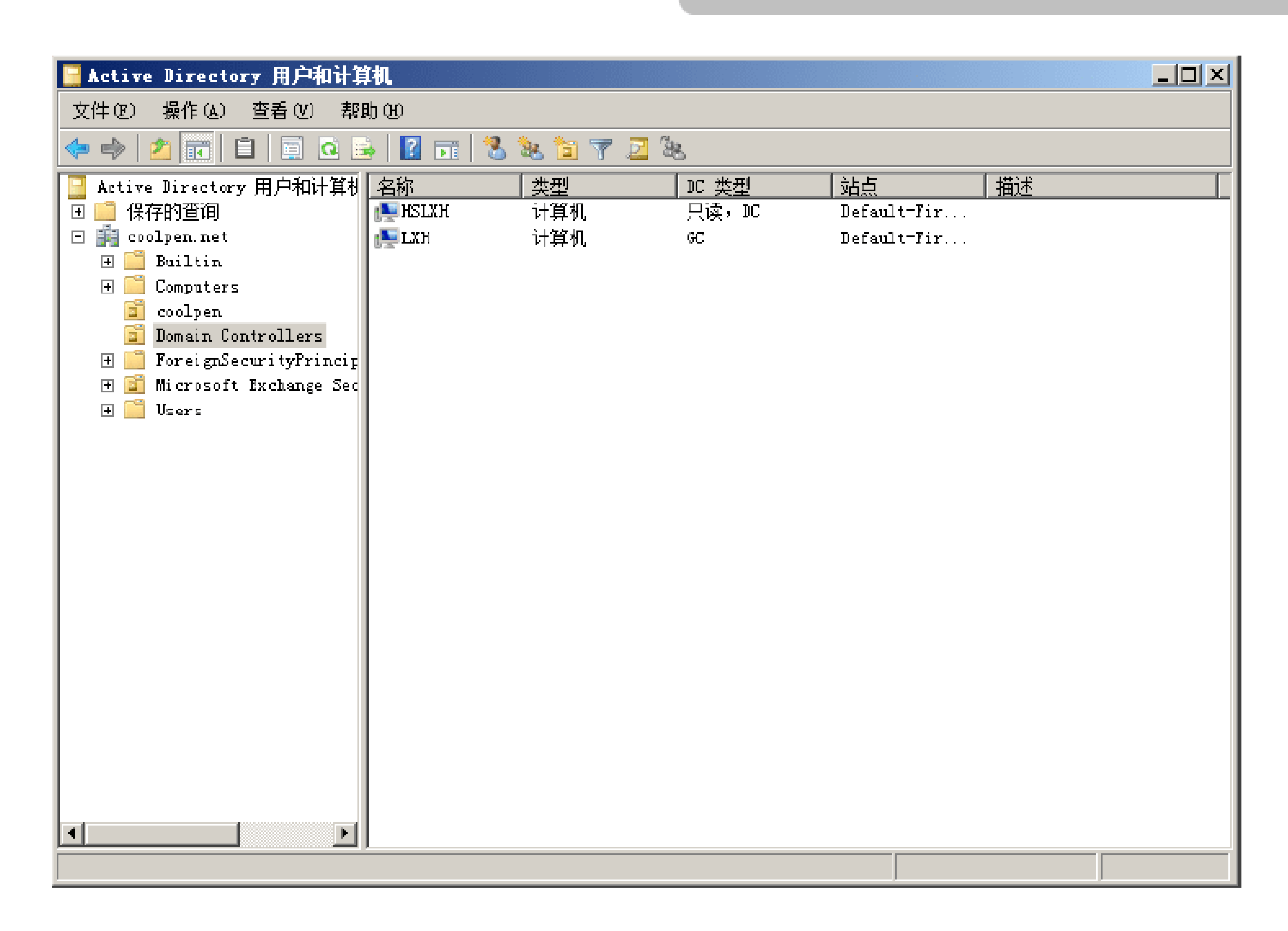


图 3-81　“Active Directory 用户和计算机”窗口

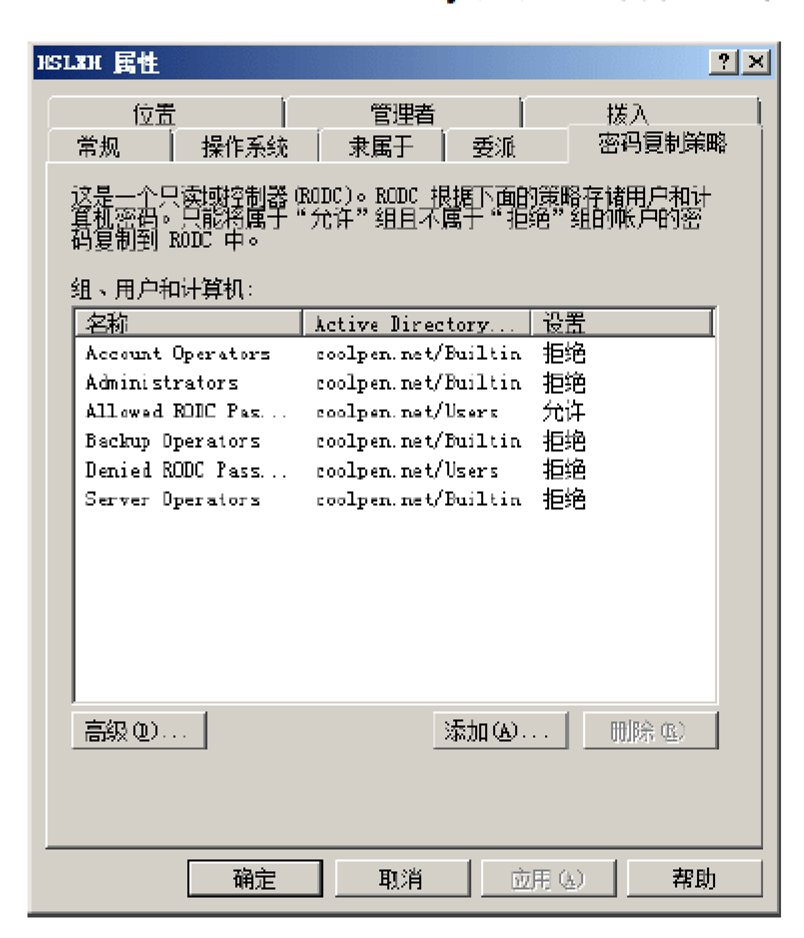


图 3-82　“密码复制策略”选项卡



提示：单击“高级”按钮，显示如图 3-83 所示的“以下项目的高级密码复制策略 HSLXH”对话框，这里显示的是密码复制策略的高级功能，用户可以根据需要选择使用。在“策略使用率”选项卡的“显示满足下列条件的用户和计算机”下拉列表中，包括如下选项：

- 选择“其密码已经存储在只读域控制器中的账户”选项，除了 RODC 自身的计算机账户和 Kerberos 票据授权(KRBTGT)账户之外，默认情况下没有缓存任何账户的密码。
- 选择“已通过此只读域控制器身份验证的账户”选项，显示在 RODC 进行身份验证的用户以及计算机，通过此列表确定允许哪些账户的密码，在此 RODC 域控制器中进行缓存。

③　单击“添加”按钮，显示如图 3-84 所示的“添加组、用户和计算机”对话框。设置 RODC 域控制器中允许或者拒绝缓存的组、用户和计算机，这里选择“允许该账户的密码复制到此 RODC 中”单选按钮。

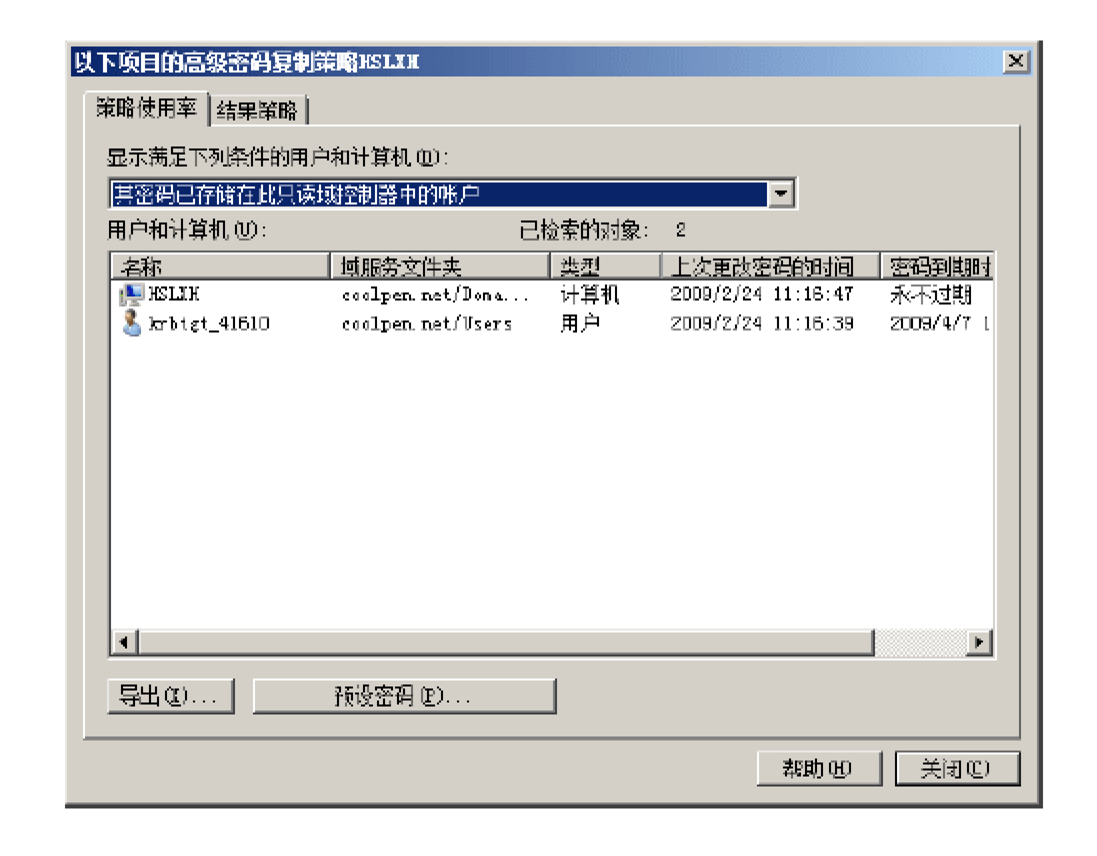


图 3-83 “以下项目的高级密码复制策略 HSLXH”对话框

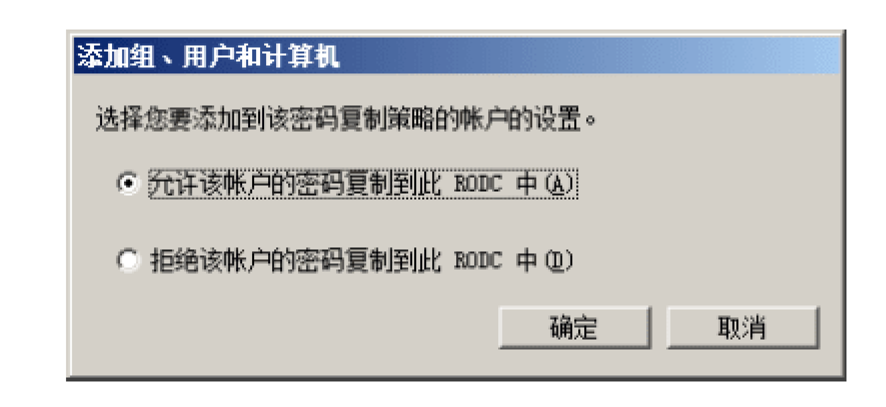


图 3-84 “添加组、用户和计算机”对话框

④ 单击“确定”按钮，显示如图 3-85 所示的“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入想要添加的域用户账户。单击“检查名称”按钮，可检查输入的用户是否正确。

⑤ 单击“确定”按钮，关闭“选择用户、计算机或组”对话框，返回到“HSLXH 属性”对话框，如图 3-86 所示，所选用户账户已被添加到列表中。



图 3-85 “选择用户、计算机或组”对话框

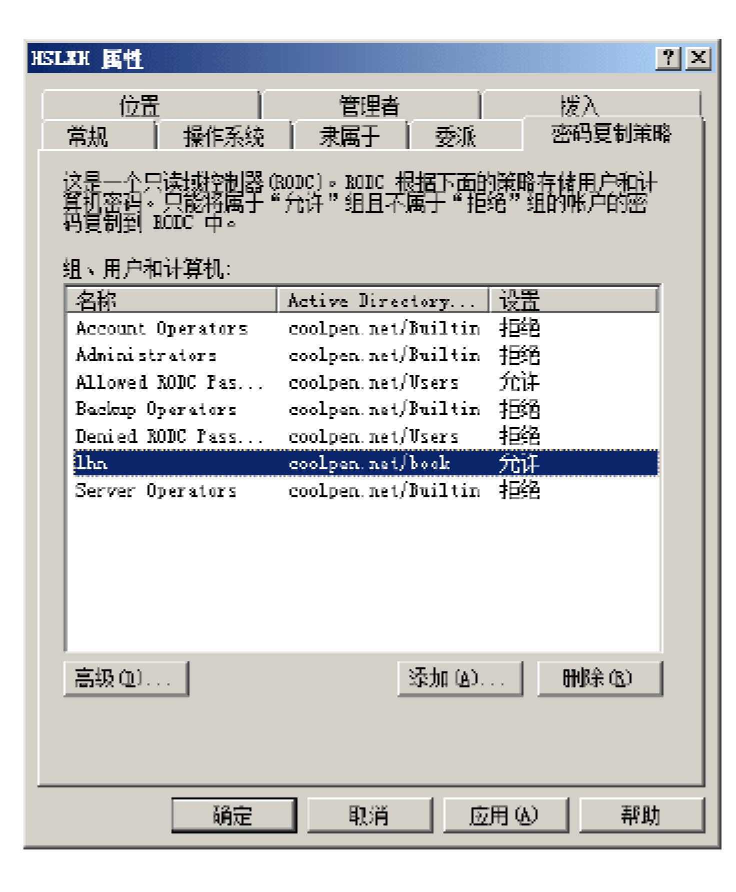


图 3-86 “HSLXH 属性”对话框

⑥ 单击“确定”按钮，保存设置即可。

3.1.7 可重新启动的活动目录域服务

在 Windows Server 2008 中，可以重启活动目录域服务，而不用重新启动域控制器，这在 Windows 2000 Server 和 Windows Server 2003 中是无法实现的，可重新启动的 ADDS 可减少执行某些操作所需的时间。通过停止 ADDS，可以将更新应用到域控制器，或执行 Active Directory 数据库脱机碎片整理等任务。

在服务器上运行不依赖于 ADDS 的其他服务，如动态主机配置协议(DHCP)，在 ADDS 停止时仍可用来满足客户端请求。可重新启动的 ADDS 具有如下优点：

- 安全更新计划者和管理员。
- ADDS 管理团队。
- AD DS 管理员。

默认情况下，可重新启动的 ADDS，在所有 Windows Server 2008 的域控制器上都是可用的。使用此功能不存在任何功能级别的要求或任何其他先决条件。

在 Windows 2000 Server 操作系统和 Windows Server 2003 操作系统的 Active Directory 中，对数据库进行脱机碎片整理时，需要在目录服务还原模式下重新启动域控制器。此外，应用安全更新通常也需要重新启动域控制器。但是在 Windows Server 2008 中，管理员可以停止并重新启动 ADDS，这样便能够更快速地执行脱机 ADDS 操作。

① 在“服务”管理窗口，双击 Active Directory Domain Services，显示如图 3-87 所示的“Active Directory Domain Services 的属性(本地计算机)”对话框。

② 单击“停止”按钮，显示如图 3-88 所示的“停止其他服务”对话框，在列表中显示了与该服务相关联的其他服务。



图 3-87　“Active Directory Domain Services 的属性(本地计算机)”对话框



图 3-88　“停止其他服务”对话框

③ 单击“是”按钮，确认停止服务即可。

若要重新启动该服务，在“Active Directory Domain Services 的属性(本地计算机)”对话框中单击“启动”按钮即可。

3.2　活动目录数据库

Active Directory 数据库是一个事务处理数据库系统，使用日志文件存储事务日志，具备“回滚”功能，确保系统发生异常的时候完成数据的入库操作。尽管如此，也应时刻做好数据库信息的备份操作，以免由于硬件损坏或其他故障导致用户信息丢失。

Active Directory 数据库相关的文件列举如下。

- Ntds.dit：数据库文件。Ntds.dit 会随着数据库的填充而不断增大。但是，日志的大小却是固定的为 10MB。对数据库进行的任何更改都会被追加到当前的日志文件中，而且其磁盘映像会不断保持更新。

- Edbxxxxx.log：事务日志文件。Edb.log 是当前的日志文件。对数据库进行更改后，将该更改写入到 Edb.log 文件中。当 Edb.log 文件充满事务之后，会被重新命名为 Edbxxxxx.log，日志文件从 Edb00001 开始，并使用十六进制累加。由于 Active Directory 使用循环记录，所以在旧日志文件写入数据库之后，这些旧日志文件会及时删除。在任何时刻都可以找到 Edb.log 文件，而且还可能有一个或多个 Edbxxxxx.log 文件。
- Edb.chk：检查点文件。Edb.chk 文件存储数据库的检查点，这些检查点标识数据库引擎需要重复播放日志的点，通常在恢复或初始化时。
- Res1.log、Res2.log：预留的日志文件。Res1.log 和 Res2.log 是磁盘空间占用文件，用来在存储日志文件的驱动器上预留最后的 20MB 磁盘空间。这是为了给日志文件提供足够的空间，以便在其他所有磁盘空间都已使用的情况下可以正常关机。



提示：为了提高 Active Directory 服务的性能和安全，建议将日志文件存储在数据库所在磁盘以外的其他磁盘上。

3.2.1 设置目录数据库访问权限

默认情况下，所有具有管理员权限的账户都可以访问目录数据库所在的文件夹。为了确保目录数据库不被恶意删除或修改，建议将该目录访问权限设置为仅有指定的用户可以访问，非授权用户禁止访问 Active Directory 数据库所在的目录。Active Directory 数据库的默认保存路径为 C:\Windows\NDTS\。

① 在 Windows 资源管理器中找到数据库文件所在的文件夹，右击 NTDS 并选择快捷菜单中的“属性”命令，打开“NDTS 属性”对话框，切换至如图 3-89 所示的“安全”选项卡。

② 在“组或用户名称”列表框中，选中需要删除的用户或组，单击“删除”按钮，即可删除选中的组或用户。通常只保留 Administrators 和 SYSTEM 组即可。

③ 单击“确定”按钮，完成访问权限的设置。

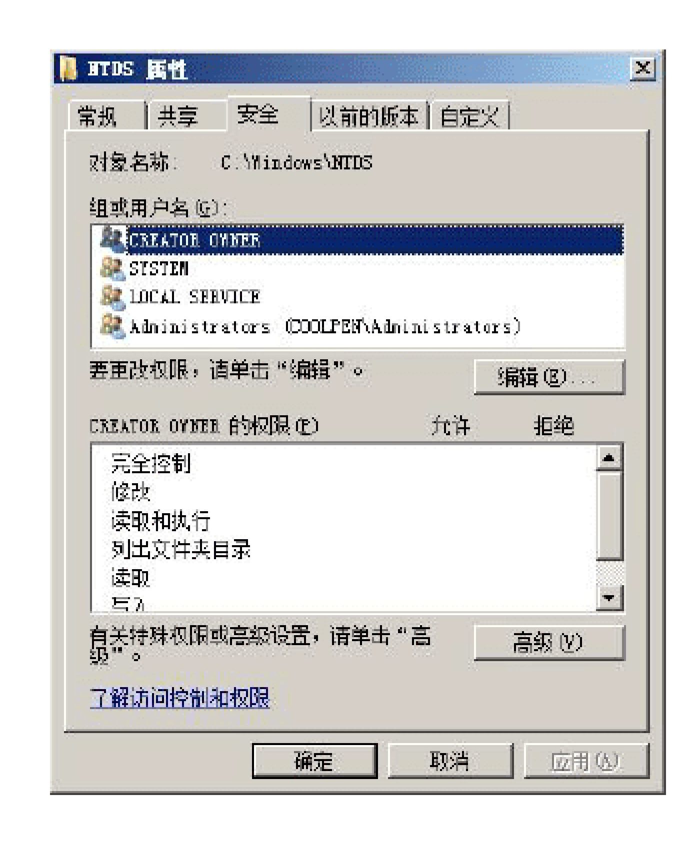


图 3-89 “安全”选项卡

3.2.2 整理活动目录数据库

为了提高活动目录在网络中的完整性、可用性，应适时对 Active Directory 数据库进行整理。活动目录整理分为两种模式：在线整理和离线整理。默认情况下，系统每隔 12 小时会自动运行一次在线整理，整理过程中需要占用比实际数据库大小更多的空间。若想减小 Active Directory 数据库的大小，则需要使用离线整理方式。使用离线整理之前，暂存需要整理的 Active Directory 数据库文件的目标驱动器中，至少需要 2 倍以上的可用空间，来暂存临时生成的 Active Directory 数据库文件。



提示：离线整理需要 Windows Shell 命令功能的支持，必须安装 Windows Server Backup 中的“命令行工具”组件。在执行离线整理过程中，需要对数据库进行完整性检测，如果数据库文件发生损坏，系统将自动做好标记。

① 在域控制器启动的时候，按下 F8 键进入启动菜单，选择“目录服务还原模式”，系统进入安全模式。

② 进入安全模式后，打开命令提示符窗口，输入如下命令：

```
ntdsutil
```

按 Enter 键，转入 ntdsutil 提示符下，显示如图 3-90 所示的结果。

③ 在 ntdsutil 提示符下输入如下命令：

```
activate instance ntds
```

按 Enter 键，显示如图 3-91 所示的结果，将 ntds 设置为活动实例。

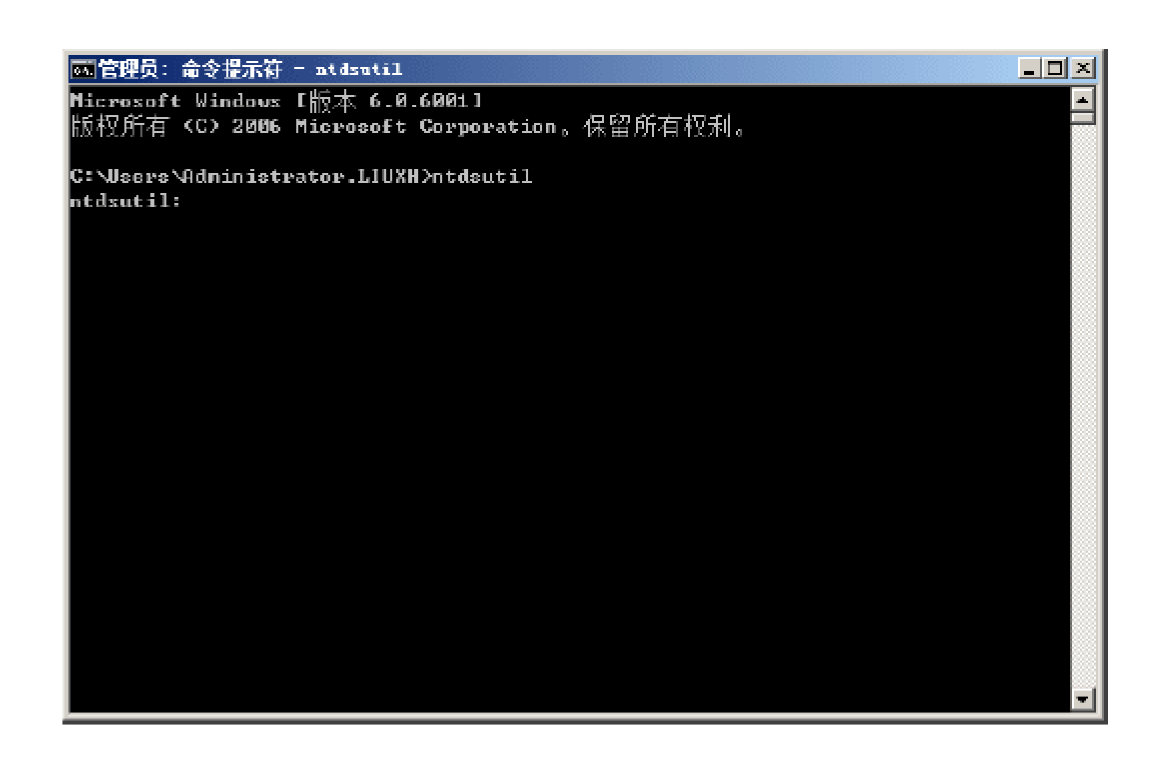


图 3-90　进入 ntdsutil 提示符下

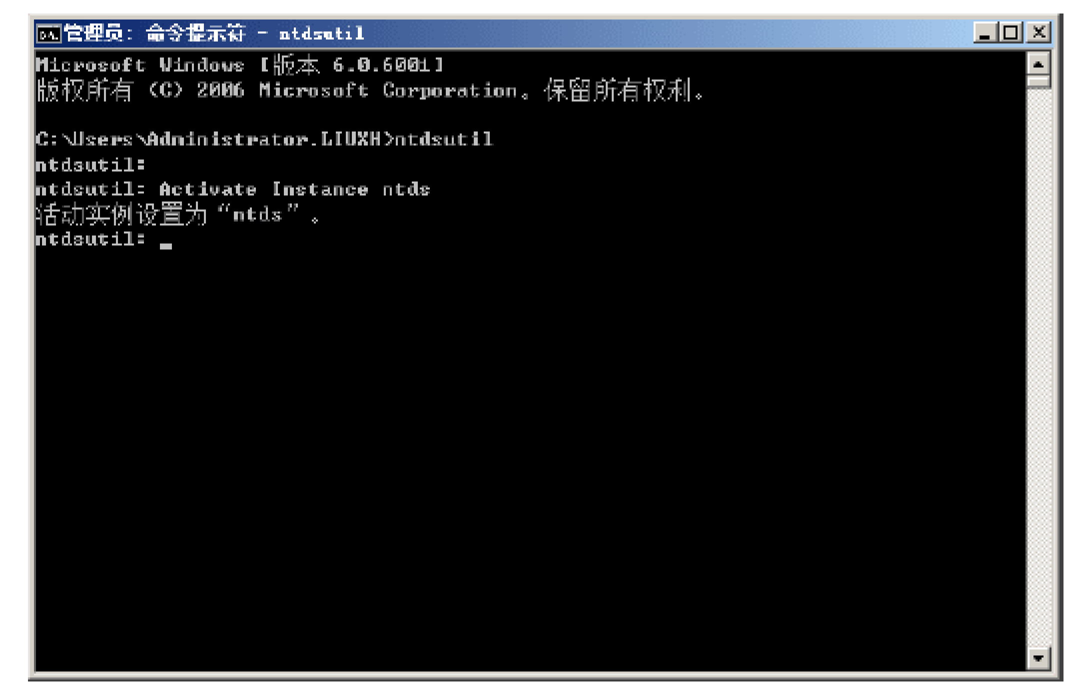


图 3-91　将 ntds 设置为活动实例

④ 在 ntdsutil 提示符下输入如下命令：

```
files
```

按 Enter 键，显示如图 3-92 所示的结果，转入 file maintenance 提示符下。

⑤ 在 file maintenance 提示符下输入如下命令：

```
info
```

按 Enter 键，显示如图 3-93 所示的结果，列出了当前使用的 Active Directory 数据库文件的位置，建议记录这些信息，最后需要用整理后的数据库重新覆盖原有数据库。

⑥ 在 file maintenance 提示符下，输入如下命令：

```
compact to c:\temp
```

按 Enter 键，显示如图 3-94 所示的结果。

⑦ 系统将在指定的 temp 目录下创建一个经过压缩的 Active Directory 数据库文件。如果输入的目录不存在，系统将会自动创建输入的目录。

⑧ 输入两次 quit 命令可返回系统命令提示符。

⑨ 使用压缩后的 Active Directory 数据库文件替换当前正在使用的数据库文件。在系统命令提示符窗口中输入如下命令：

```
copy "c:\temp\ntds.dit" "C:\WINDOWS\NTDS\ntds.dit"
```

按 Enter 键，提示是否要覆盖原有文件，输入“yes(y)”或“all(a)”确认覆盖，显示如图 3-95 所示的结果。

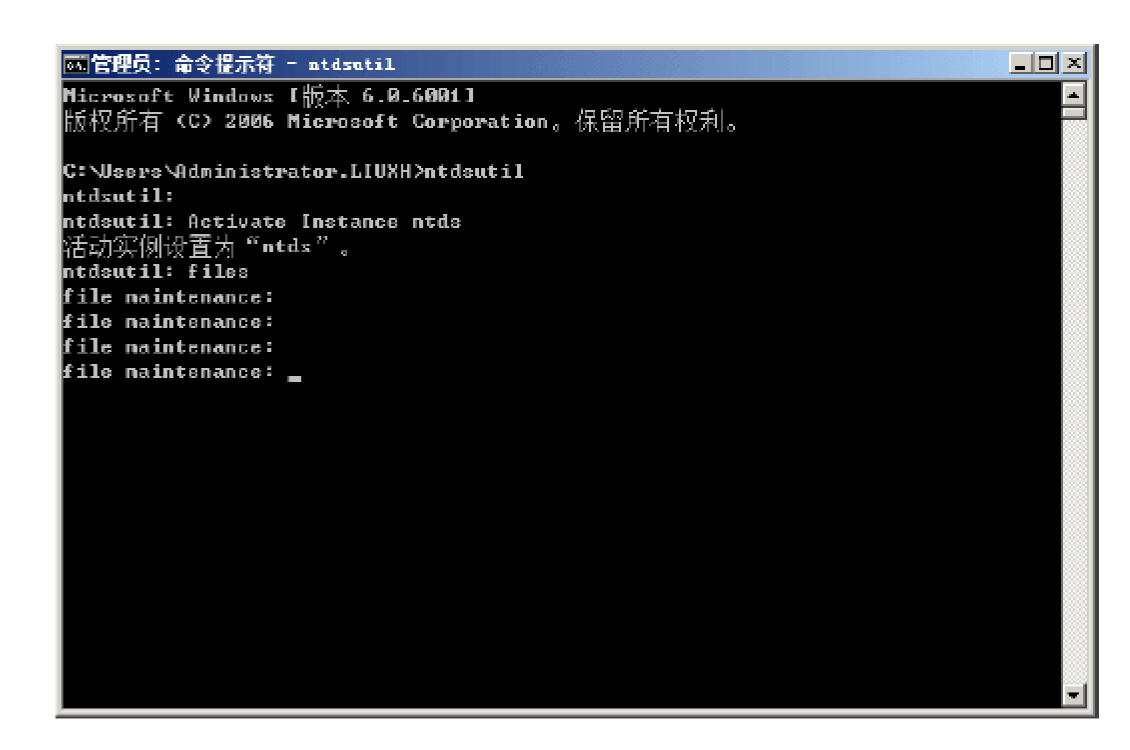


图 3-92 转入 file maintenance 提示符

图 3-93 当前数据库信息

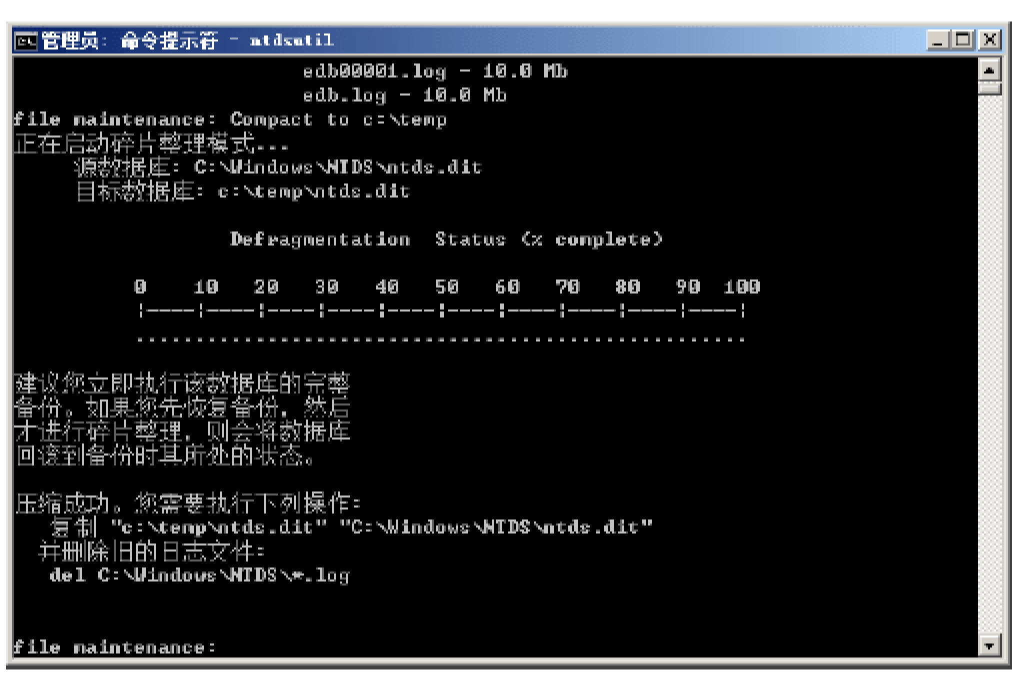


图 3-94 压缩数据库文件

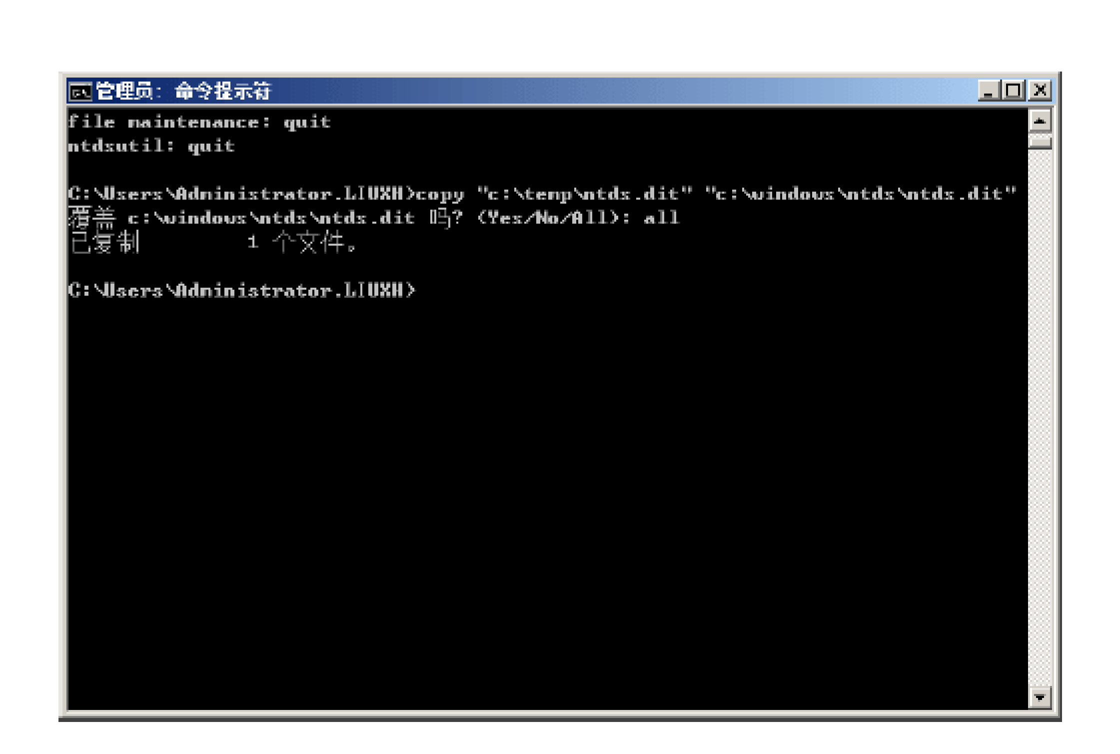


图 3-95 Active Directory 数据库文件替换

⑩ 继续输入如下命令：

```
del C:\WINDOWS\NTDS\*.log
```

按 Enter 键，删除 Active Directory 数据库文件目录下所有的 LOG 文件，显示如图 3-96 所示的结果。

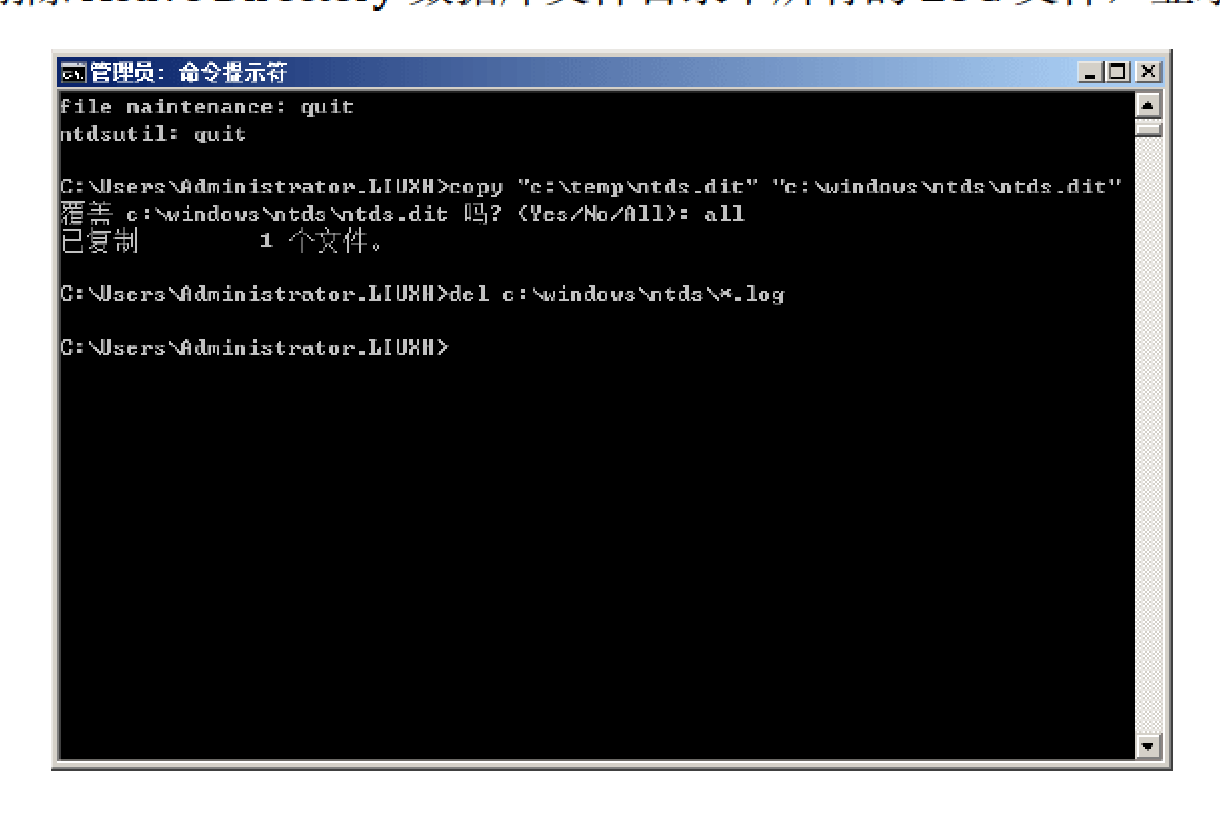


图 3-96 删除日志文件

⑪　重新启动域控制器，正常登录即可。

3.2.3　重定向活动目录数据库

活动目录的数据库包含了大量的核心信息，应该妥善保护，并且随着时间的推移，信息量也会不断增加。当数据库所在分区空间不足时，可能导致原有信息丢失或残缺，此时应及时删除原有信息，或重新定向活动目录库的存储目录。另外，如果安装 Active Directory 时，将数据库文件保存在系统默认的位置，则很容易被攻击者入侵。为确保数据库信息的安全，应将其保存到一个相对安全的位置。



提示：活动目录的数据库文件包括 Ntds.dit、Edb.log、Temp.edb。

重定向 Active Directory 数据库位置的主要操作步骤如下。

①　以“目录服务还原模式”启动服务器，进入安全模式后，打开命令提示符窗口，输入 Ntdsutil 命令并执行，转入 ntdsutil 提示符下。继续输入 files 命令并执行，转入 file maintenance 提示符下。

②　在 file maintenance 提示符下输入如下命令：

```
move db to d:\AD-db
```

按 Enter 键运行，将 Active Directory 数据库重定向到 d:\AD-db 目录下，显示如图 3-97 所示的结果。

```
管理员: 命令提示符 - ntdsutil
ntdsutil: files
file maintenance: move db to d:\AD-db

已成功更新备份排除项。
正在从 C:\Windows\NTDS 拷贝 NTFS 安全性到 d:\AD-db...
上一个 NTDS 数据库位置 C:\Windows\NTDS\dsadata.bak 不可用。将应用默认的 NTFS 安
全性到 NTDS 文件夹。
重新启动时将在 NTDS 文件夹上设置默认 NTFS 安全性。
正在从 C:\Windows\NTDS 拷贝 NTFS 安全性到 d:\AD-db...

驱动器信息:

        C:\ NTFS (硬盘) 空白(21.2 Gb) 总共(29.2 Gb)
        D:\ NTFS (硬盘) 空白(10.6 Gb) 总共(10.7 Gb)

DS 路径信息:

        数据库    : d:\AD-db\ntds.dit - 12.1 Mb
        备份目录 : d:\AD-db\DSADATA.BAK
        工作目录: d:\AD-db
        Log dir     : C:\Windows\NTDS - 30.0 Mb total
                        edbres00002.jrs - 10.0 Mb
                        edbres00001.jrs - 10.0 Mb
                        edb.log - 10.0 Mb

移动数据库成功。
请立即进行备份，否则将无法
还原新文件位置。
file maintenance: _
```

图 3-97　重定向活动目录数据库

③　在 file maintenance 命令提示符下，输入如下命令：

```
move log to d:\AD-db
```

按 Enter 键，将 AD 数据库日志重定向到 d:\AD-db 目录下，显示如图 3-98 所示的结果。

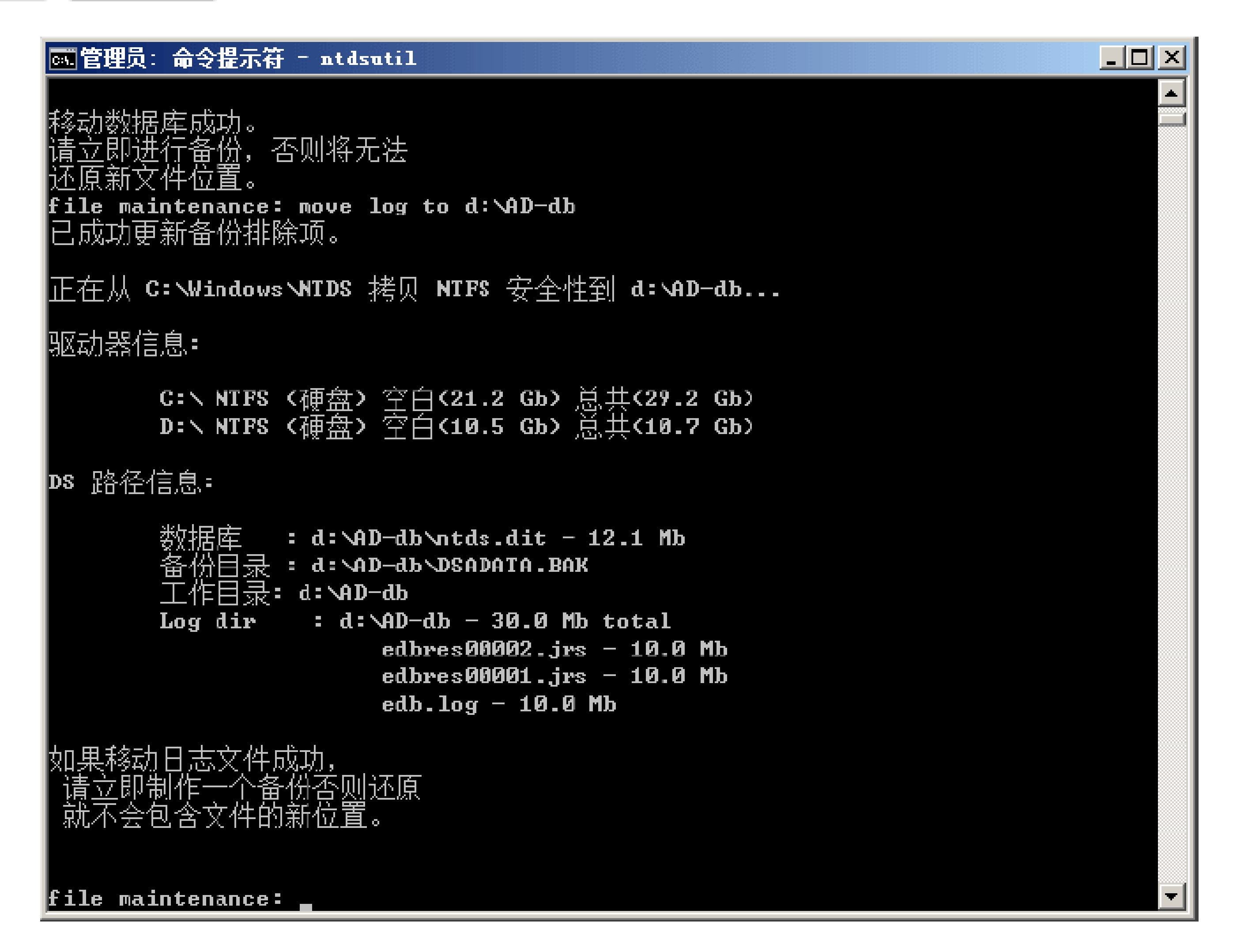


图 3-98　重定向活动目录数据库日志

④　命令成功执行，使用 quit 命令返回系统命令提示符即可。

第 4 章　组策略安全

组策略是从 Windows 2000 系统开始就集成的默认组件，通常用作系统和网络安全管理。允许管理员对所辖用户账户或组权利进行设置，并且可以将对象指定的操作权限赋予特定的用户账户。在域环境中，则允许管理员对所有域用户账户进行管理、管理工作站的安全设置等。Windows Server 2008 系统的组策略功能更加强大，安全策略更加丰富，可以为管理员提供更加详细的网络管理功能。

关键词

- 组策略概述
- 编辑组策略
- 安全策略
- 软件限制策略
- IE 安全策略

4.1 组策略概述

在 Windows 2000/XP/2003 系统中，策略模板文件一直使用单独文件格式，即.adm 文件。传统的.adm 模板文件虽然为修改注册表提供了必要的方法，但也有诸多不便之处，例如版本控制、多语言支持等。在 Windows Server 2008 系统中，采用了全新文件格式的策略模板，即.admx，新策略模板文件的出现，使 Windows Vista 或 Windows Server 2008 用户管理基于注册表的策略设置变得更加简便。

4.1.1 Windows Server 2008 中组策略的新特性

在 Windows Server 2008 系统中，对原有的系统策略进行了扩展，Windows Server 2003 SP1 中提供了约 1700 条组策略设置，但是在 Windows Server 2008 系统中已增加至 2400 条组策略，管理功能更加丰富。在 Windows Server 2008 系统中，组策略管理控制台提供了更多元化的组策略管理方式，主要有以下新特点：

- 支持新的策略应用范围，包括无线和有线网络，Windows 防火墙和 IPSec 策略，支持电源管理和 USB 设备限制策略。
- 客户和域控制器之间慢速链接检测已经有所改进，现在可以有一个更稳定的机制，来判定客户是否通过慢速链接连接到域控制器，从而决定所应用的组策略行为。
- 组策略更新现在是基于域控制器的可用性，也就是说，当客户远程通过 VPN 链接到网络的时候，组策略更新会更加及时。
- 支持多个本地策略对象(LGPO)以及针对不同的用户组或用户设置不同的组策略对象。
- 支持基于 XML 的管理模板文件格式化(ADMX)，更好地支持多语言模板。
- 支持 per-GPO 和 per-GP 的设置。
- GPMC 和组策略编辑器都有了改进，并且增加了新功能。
- 增加了通过收购 Desktop Standard 所获得的工具，也就是现在被称为 Group Policy Preferences 的工具，用它来实现组策略的自动创建。

4.1.2 ADMX 和 ADM 文件

新的 ADMX 文件格式和自 Windows NT 4.0 起便存在的旧 ADM 格式最大的区别在于，ADMX 采用了 XML 标准来描述注册表策略的设置。首先，编辑 XML 的工具要远多于编辑 ADM 语法的工具。其次，由于 XML 是架构化的，因此最终会比较容易构建一些工具，来帮助您在正确位置放置正确的标记，进而创建结构良好的 ADMX 文件。其中架构化是指，对于给定的 XML 应用程序(如 ADMX 格式)，有一个文档化的架构来描述可能用到的元素和属性以及它们的组织方式。后面的部分将对一个示例进行分析。

1. ADMX 和 ADM 文件的区别

ADMX 和 ADM 的另一个主要区别在于，主 ADMX 文件的字符串部分划分到了语言特定的 ADML(ADM Language，ADM 语言)文件中。如果熟悉 ADM 文件，就会知道每个文件的结尾会有一个以“[strings]”标记分隔的部分，其中用户可以为字符串赋值，该字符串会在使用组策略编辑器和管理模板时显示。例如，单击给定策略的“解释”选项卡时所看到的文本，就存储在该字符串部分中。问题是，字符串存储在 ADM

文件中，如果希望在其他语言的 Windows 系统上使用该 ADM，则需要创建一个新的 ADM 文件，并加上适用于该语言的字符串部分。

ADM 文件本身默认被保存在组策略的 SYSVOL 目录下的“组策略模板”中，因此，每当创建一个 GPO，就会在每个域控制器上占用大约 4MB 的存储空间。并且，组策略模板对于在其他工作站上编辑组策略都是必不可少的，没有相应的 ADM 文件，就无法编辑包含在 GPO 内的任何自定义设置。使用 ADMX 格式，就可以避免这些问题。用户不必再将任何内容直接存储在 GPO 内部，因此不会出现通常所说的“SYSVOL 膨胀”。新 ADMX 标准可以利用“中心库”所具备的优势存储新的 ADMX 文件，而不必将它们复制到每个 GPO 中。“中心库”的另一重要作用是：如果 ADMX 文件具有更新的定义，则所有管理工作站将立即使用更新的 ADMX 文件。

新的 ADMX 和 ADML 文件同样具有新的存储模型，在 Windows Server 2008 系统中的默认存储路径是%windir%\policydefinitions，如图 4-1 所示。

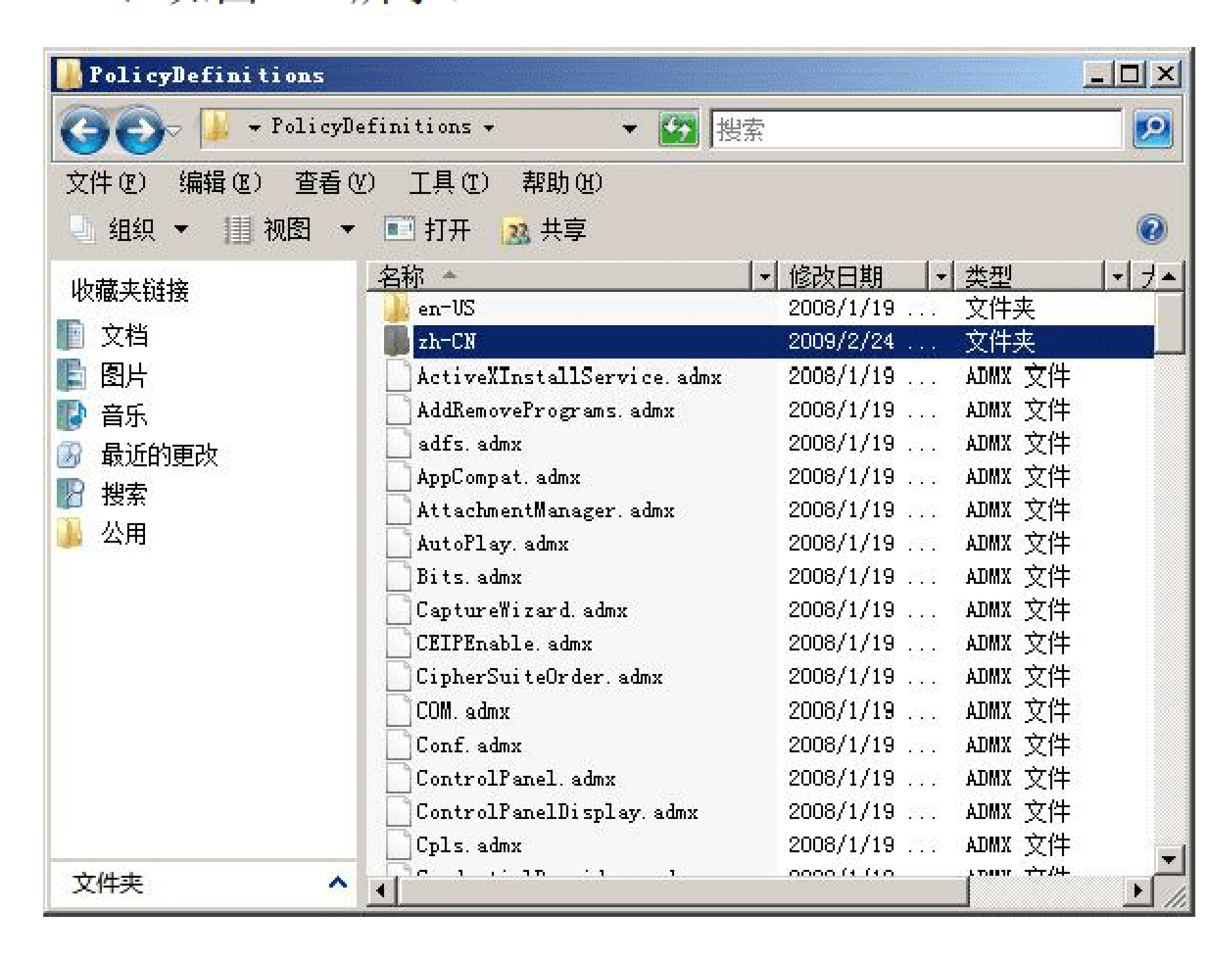


图 4-1　查看 Windows Server 2008 中的 ADMX 文件

ADMX 文件存储目录下的 en-US 和 zh-CN 文件夹分别用于存储中文和美式英语的 ADML 文件。当启动组策略编辑器，展开管理模板节点的时候，编辑器会自动查找到%windir%\policydefinitions 文件夹。当然也可以把这些文件复制到中央位置，例如中央存储。

中央存储是在 SYSVOL 中创建的域范围的目录，降低因 GPO 数量的不断增加而导致的其他存储和更大复制通信的需求。创建中央存储之前，组策略管理工具使用本地计算机中的核心操作系统 ADMX 文件。此外，管理工具还可以读取在本地存储或在 GPO 中存储的任何其他 ADM 文件。这将确保不同平台管理之间的互操作性。仅存在于 ADMX 文件中的所有策略设置只能在平台中使用。

ADMX 和 ADML 文件不会自动复制到 GPO 的 SYSVOL 中。如果创建一个新的 GPO，则默认不会包含任何的 ADMX 文件。所有的 ADMX 和 ADML 文件都是编辑 GPO 的时候添加进去的。这样可以节省域控制器中 SYSVOL 的存储空间，因为临时文件不再存储于每个域控制器上了。

2. ADMX 的中央存储

Windows Vista 和 Windows Server 2008 中的一个显著特性，就是 ADMX 中央存储。在先前版本的 Windows 系统中，ADM 模板的主要功能就是生成组策略的管理模板，并且自动复制到每个 GPO 模板，这

种复制机制必然产生一些问题，导致 GPO 的管理和版本控制出错。在 Windows Server 2008 和 Windows Vista 系统中，管理模板文件被基于 XML 的文件格式取代，并且增加了多语言支持和强版本控制，可以在多语言环境中管理组策略。

为了解决 ADM 模板的复制和管理问题，ADMX 文件被集中在中央存储。管理员只需要在每个域控制器的 C:\Windows\ Sysvol\sysvol\<domain name>\Policies 下创建一个名为 PolicyDefinitions 的文件夹，并将所有的 ADMX 文件复制到该文件夹中即可。

4.1.3 编辑 ADMX 模板

相对于以前操作系统版本所使用的 ADM 文件，Windows Vista/2008 中的 ADMX 格式有了明显的改进。XML 的使用为编辑和搜索这些文件提供了更为清洁的框架。语言特定字符串向单独文件的转换，使得多语言组策略编辑能够无缝地进行，同时，中心库消除了将所有 GPO 与 ADM 文件的副本一同存储并更新的必要性。用 XML 编写 ADMX 的确是一大进步，但是，许多管理员并不知道如何编写 XML，更不用说了解 ADMX 用于创建策略扩展的架构了。管理员可以使用多种编辑工具打开或编辑 ADMX 或 ADML 文件，如记事本、文本编辑器、Visual Studio 等，甚至在 IE 浏览器中就可以查看文件的详细内容。如图 4-2 所示为在记事本中打开的系统默认 XML 文件。

IndependentRolesLoc.xml - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?xml version="1.0" encoding="utf-16"?>
<!--Version 2.2-->
<SCWLocalization CultureName="en-US">
    <RoleLocalization>
        <Role Name="Core">
            <DisplayName>Core</DisplayName>
            <Description>Services required for all roles.</Description>
        </Role>
        <Role Name="SecurityandNetwork">
            <DisplayName>Security and Network</DisplayName>
            <Description>Enables network infrastructure and security services.</Description>
        </Role>
        <Role Name="Independent">
            <DisplayName>Independent</DisplayName>
            <Description>The independent role consists of Windows services that cannot be en
        </Role>
    </RoleLocalization>
    <ServiceLocalization>
        <Service Name="Appinfo">
        </Service>
        <Service Name="DcomLaunch">
        </Service>
        <Service Name="Dhcp">
        </Service>
        <Service Name="Eventlog">
        </Service>
        <Service Name="EventSystem">
        </Service>
        <Service Name="PlugPlay">
```

图 4-2 使用记事本打开 XML 文件

4.2 编辑组策略

在 Windows Server 2008 中，GPMC 被包含在基础设置中，而不用单独安装。尽管组策略对象编辑器和 GPME 的大部分功能是相同的，但是组策略对象编辑器已经被 GPME 所取代。组策略管理编辑器允许直接编辑组策略，以及配置影响计算机和用户的设置。在“组策略管理”窗口中，右击任意组策略，然后选择“编辑”选项，即可打开“组策略管理编辑器”窗口，如图 4-3 所示。

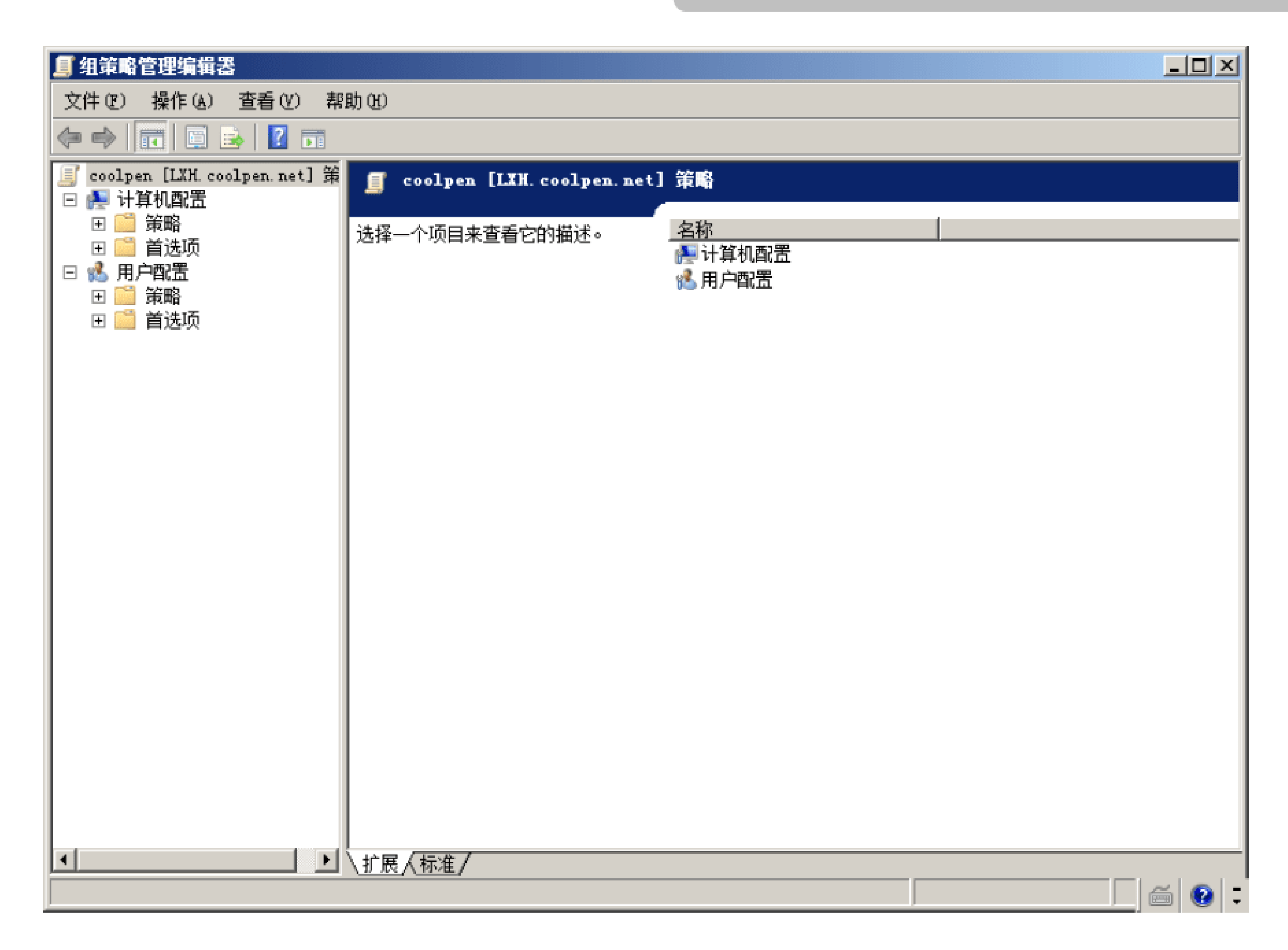


图 4-3　“组策略管理编辑器”窗口

4.2.1　管理设置

可以管理的设置有很多种，根据设置的功能不同，会出现不同的配置选项。基本的设置，包括简单的启用或禁用选项，如图 4-4 所示。高级的设置，还包括允许配置将要使用的值，如图 4-5 所示。

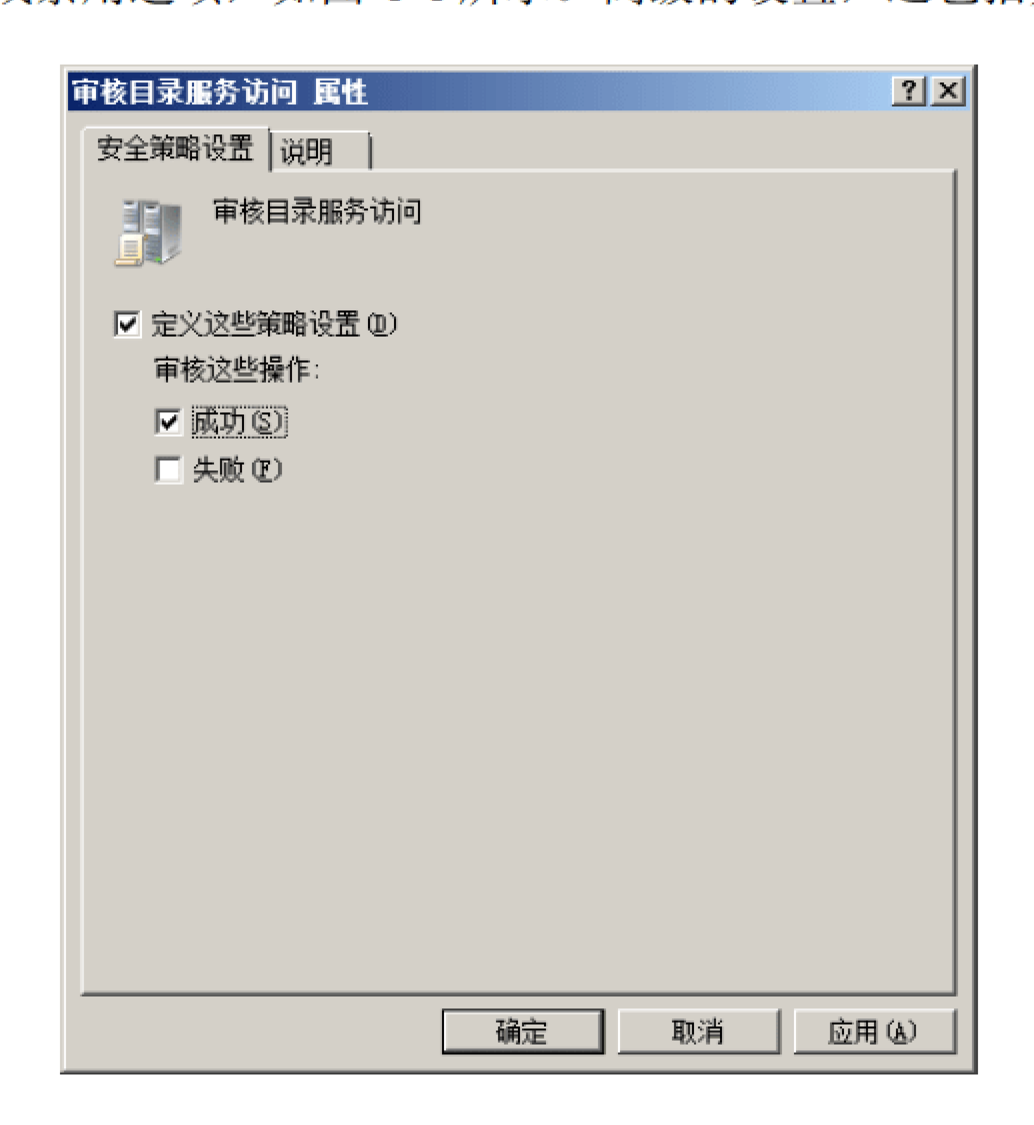


图 4-4　包括简单选项的策略



图 4-5　包括高级设置的策略

4.2.2 添加管理模板

每次评估 GPO 时，也会评估 GPO 内的所有设置，以确定如何影响用户或计算机。评估的设置越多，计算机启动或用户接收到登录对话的时间也就越长。因此，默认情况下，并没有将所有可用的管理模板全部添加在组策略结构中。换句话说，在实际使用中，只需要添加所必需的管理模板即可。

在“组策略管理编辑器”窗口中，右击“管理样板”，在快捷菜单中选择“添加/删除样板”命令。显示如图 4-6 所示的“添加/删除模板”对话框，单击“添加”按钮，浏览并选择所要添加的模板即可。

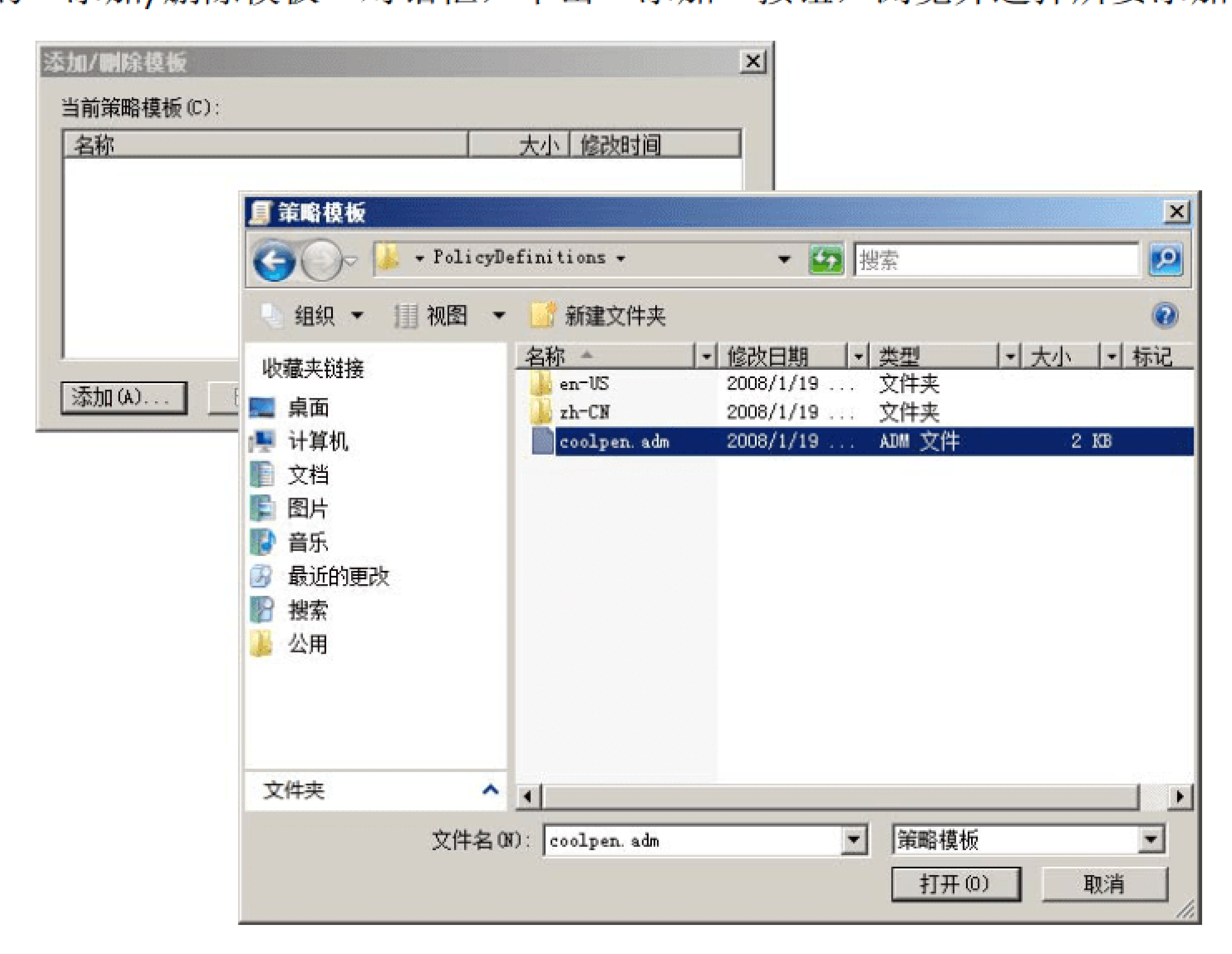


图 4-6 添加模板

4.2.3 筛选管理模板

如果对组策略设置不是很熟悉，在设置组策略时，因为可配置的设置很多，所以查找起来可能会比较困难。为了解决这个问题，在组策略管理器中，可以使用筛选功能，筛选掉所有不匹配的选项。

① 右击“计算机配置”或“用户配置”管理模板下的任一容器，在快捷菜单中选择“筛选器选项”命令，显示如图 4-7 所示的“筛选器选项”对话框。根据需要，设置所要筛选的类别。例如选中“启用需求筛选器”复选框，并在列表中选中“Windows Server 2008 家族”和“Windows Vista 家族”复选框。

② 单击“确定”按钮，保存筛选配置。

③ 再次右击模板节点，在快捷菜单中选择“打开筛选器”命令，即可启动筛选器，如图 4-8 所示为筛选后的结果。此时，根据需要设置策略模板即可。

筛选器的缺点是只能应用在管理模板上，组策略其他区域的设置不会受到影响，也不会被筛选掉。但是，这些设置被更新和修改的频率不如管理模板。

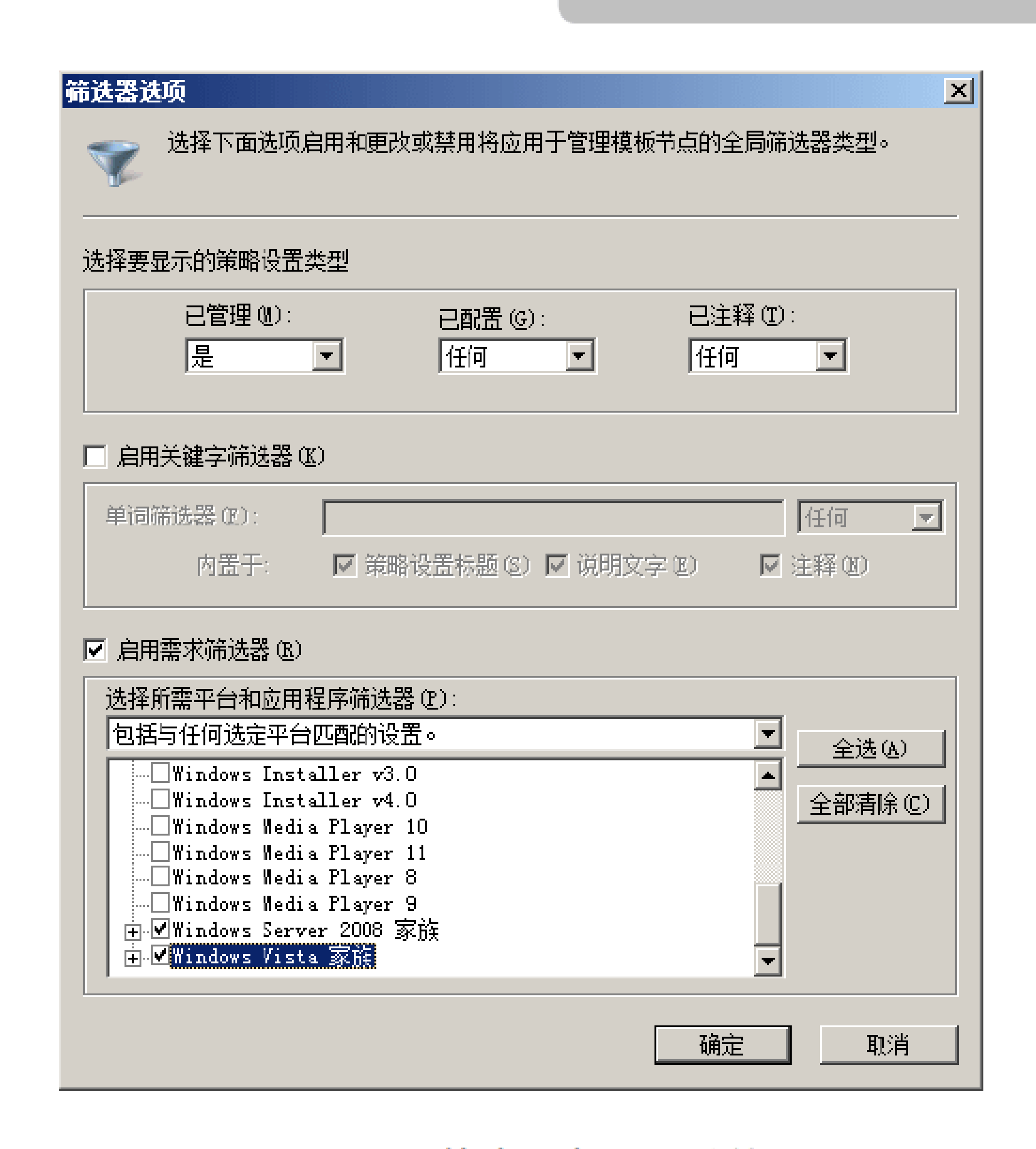


图 4-7　“筛选器选项”对话框

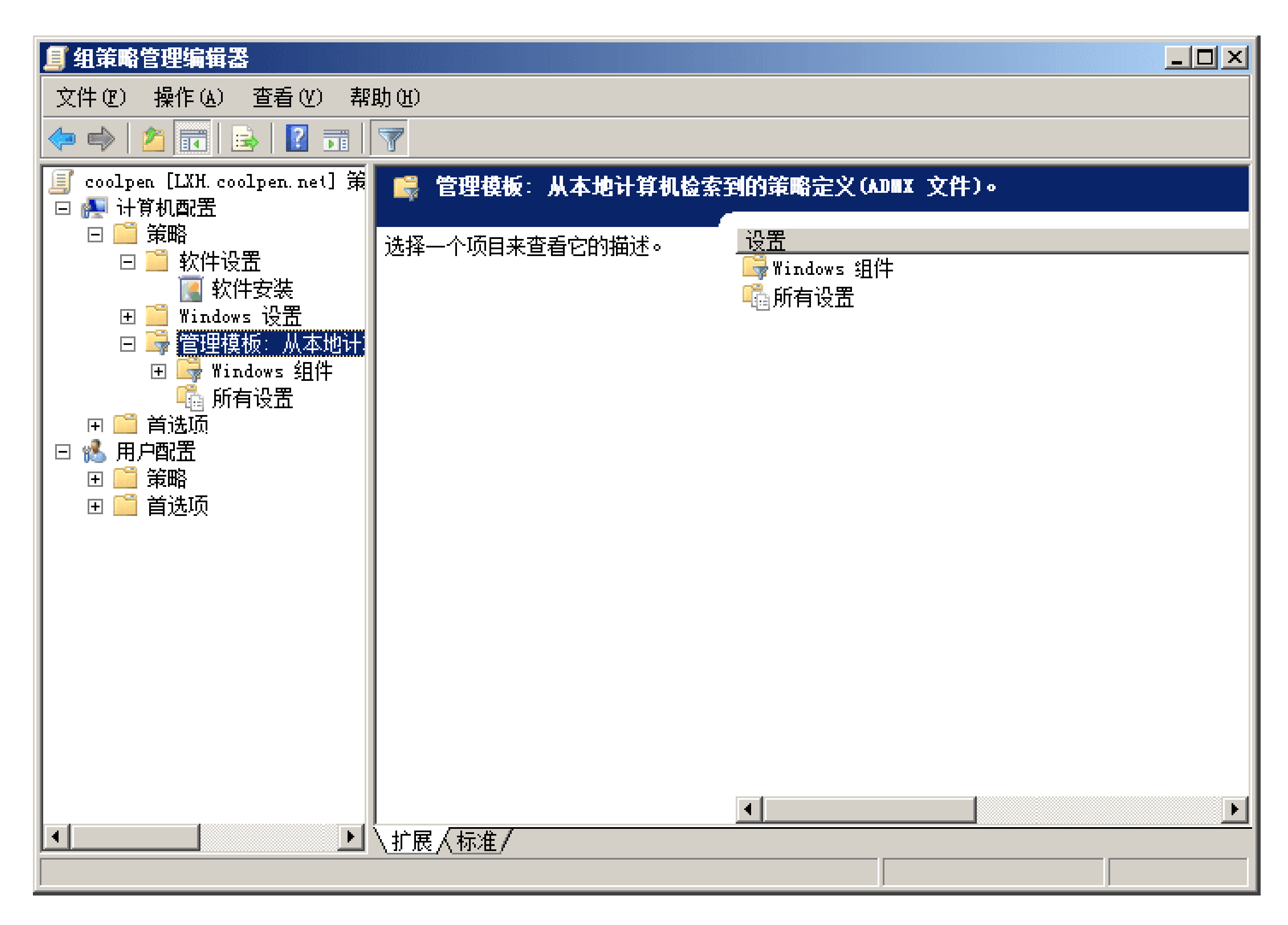


图 4-8　筛选后的管理模板

4.3　安 全 策 略

所有安全策略都是基于“计算机配置”的策略，与本地计算机上的用户账户或登录计算机的域用户账户无关。Windows Server 2008 系统的安全机制更为强大，但默认情况下并未配置，因此起不到任何保护作用，必须根据需要启用并配置这些安全策略，以确保系统安全。打开“本地组策略编辑器”窗口，并依次展开“本地计算机 策略”→“计算机配置”→“Windows 设置”→“安全设置”选项，即可开始配置相应的策略，如图 4-9 所示。

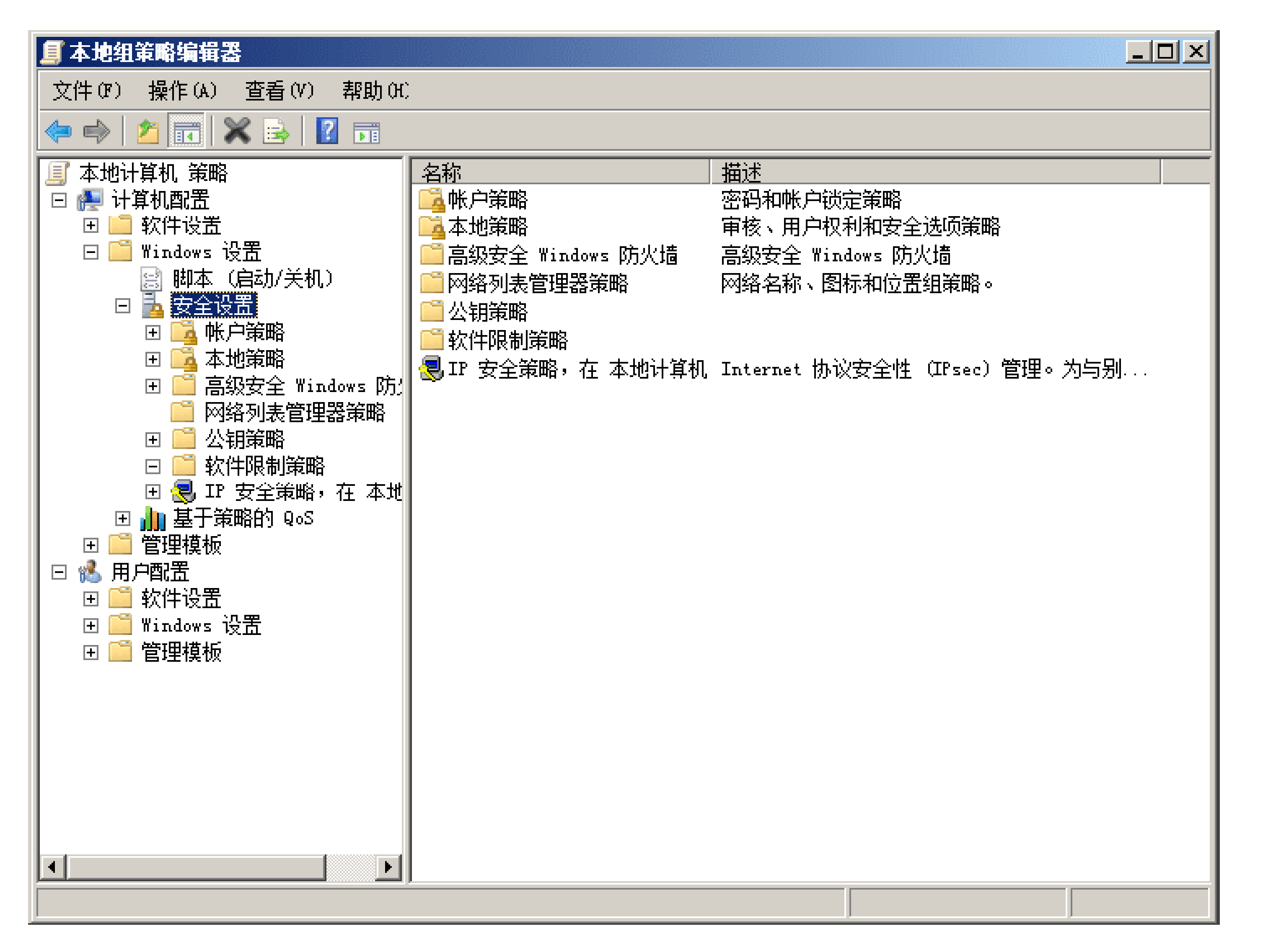


图 4-9 “本地组策略编辑器”窗口

4.3.1 账户策略

账户策略主要用于限制用户账户的交互方式，其中包括密码策略和账户锁定策略，这些设置同时适用于独立服务器和域环境。密码策略用于保护域或本地用户账户的密码安全，设定密码规则等；账户锁定策略用于保护域或本地用户账户的登录安全，确定某个账户被锁定在系统之外的情况和时间长短。

1. 密码策略

在 Windows Server 2008 系统中，默认已经为所有用户账户启用了密码策略，包括：

- 密码必须符合复杂性要求。
- 最短密码长度最小值。
- 密码最短使用期限。
- 密码最长使用期限。
- 强制密码历史。
- 用可还原的加密来储存密码。

① 双击“密码必须符合复杂性要求”策略，显示如图 4-10 所示的对话框，选择“已启用”单选按钮，即可启用该策略，最后单击“确定”按钮保存。此安全设置确定用户账户密码是否必须符合复杂性要求，如果启用此策略，密码必须符合下列最低要求。

- 不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分。
- 至少有 6 个字符长。
- 包含以下 4 类字符中的 3 类字符。
  - 英文大写字母(A～Z)
  - 英文小写字母(a～z)
  - 10 个基本数字(0～9)
  - 非字母字符(例如!、$、#、%)

- 在更改或创建密码时执行复杂性要求。

② 双击“密码长度最小值”策略，显示如图 4-11 所示的对话框，在“密码必须至少是××个字符”微调框中，设置密码的最小长度，例如 10。最后单击“确定”按钮保存。此安全设置确定用户账户密码包含的最少字符数，可选值范围为 1～14，如果直接设置为 0，则表示允许不设置密码。在 Windows Server 2008 系统中，独立服务器的默认值为 0，而域控制器默认值为 7。

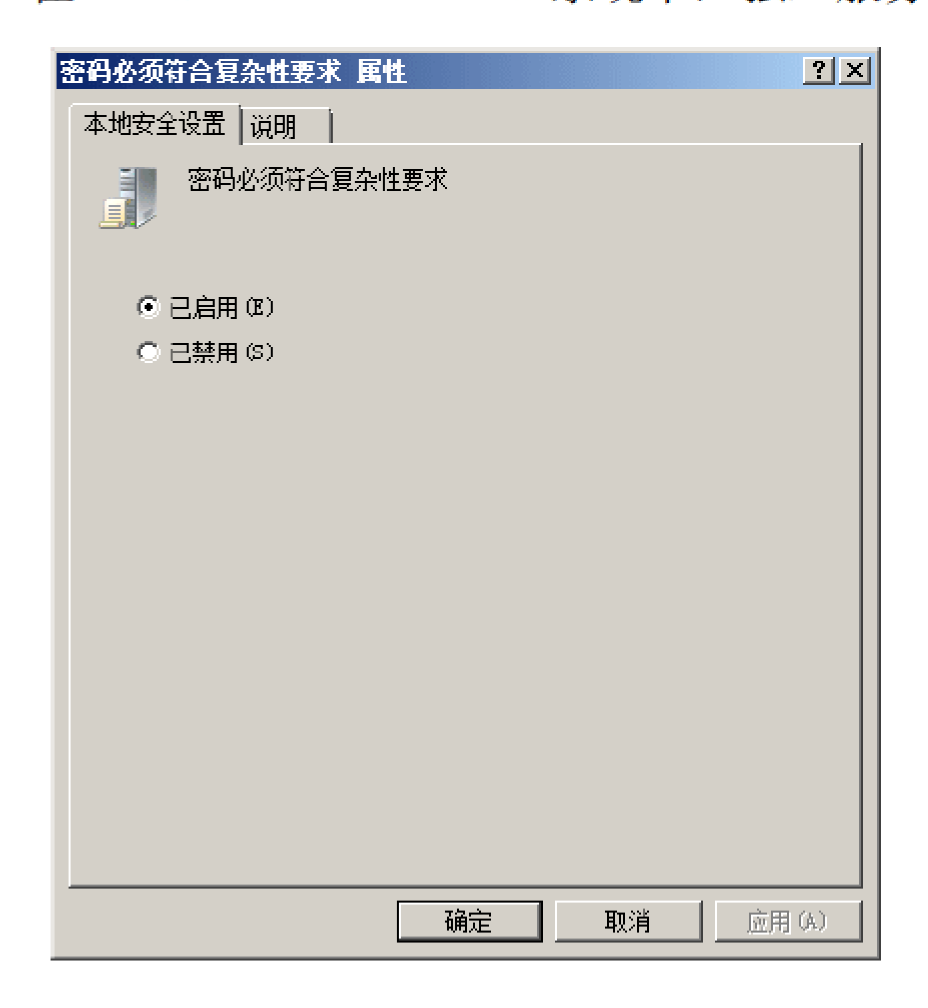


图 4-10　“密码必须符合复杂性要求 属性”对话框

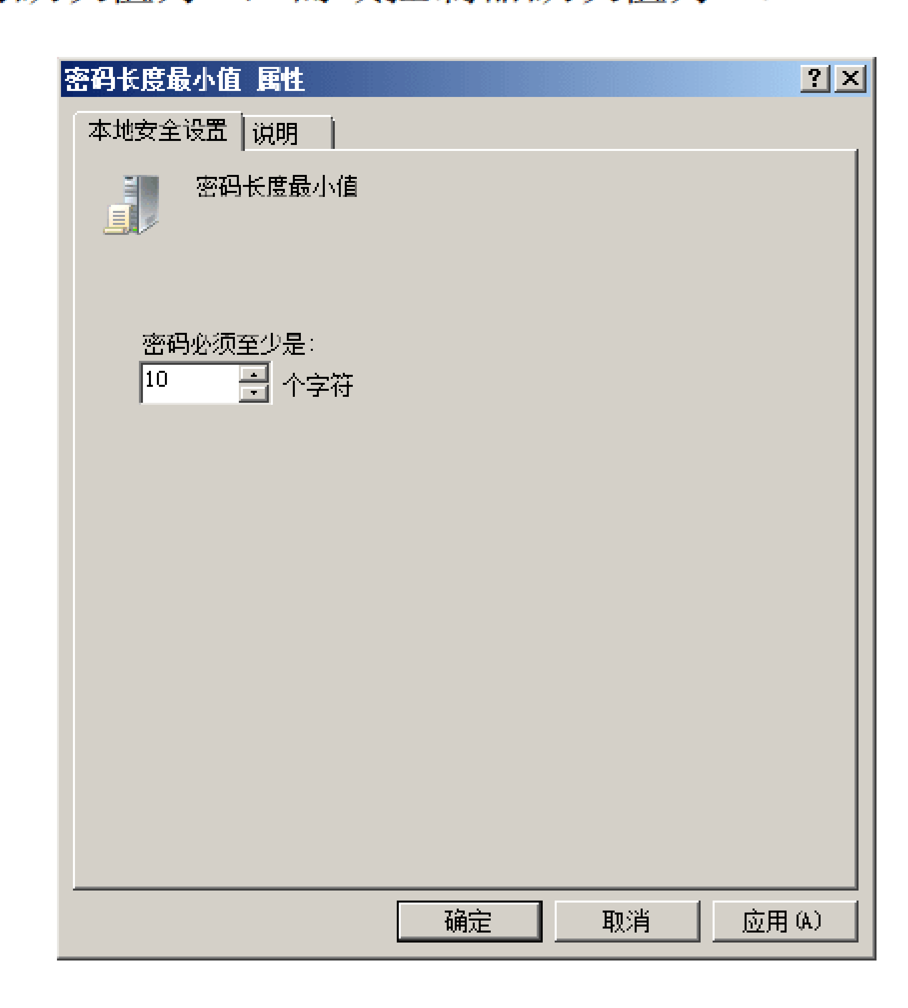


图 4-11　“密码长度最小值 属性”对话框

③ 双击“密码最短使用期限”策略，显示如图 4-12 所示的对话框，Windows Server 2008 系统的独立服务器默认值为 0，域控制器默认值为 1 天。在“在以下天数后可以更改密码”微调框中，输入相应天数(如 2 天)，单击“确定”按钮保存即可。

④ 双击“密码最长使用期限”策略，显示如图 4-13 所示的对话框，系统默认“密码过期时间”为 42 天，可选值范围为 1～999 天，如果直接设置为 0，则表示密码永不过期。Windows Server 2008 系统的默认值为 42 天。

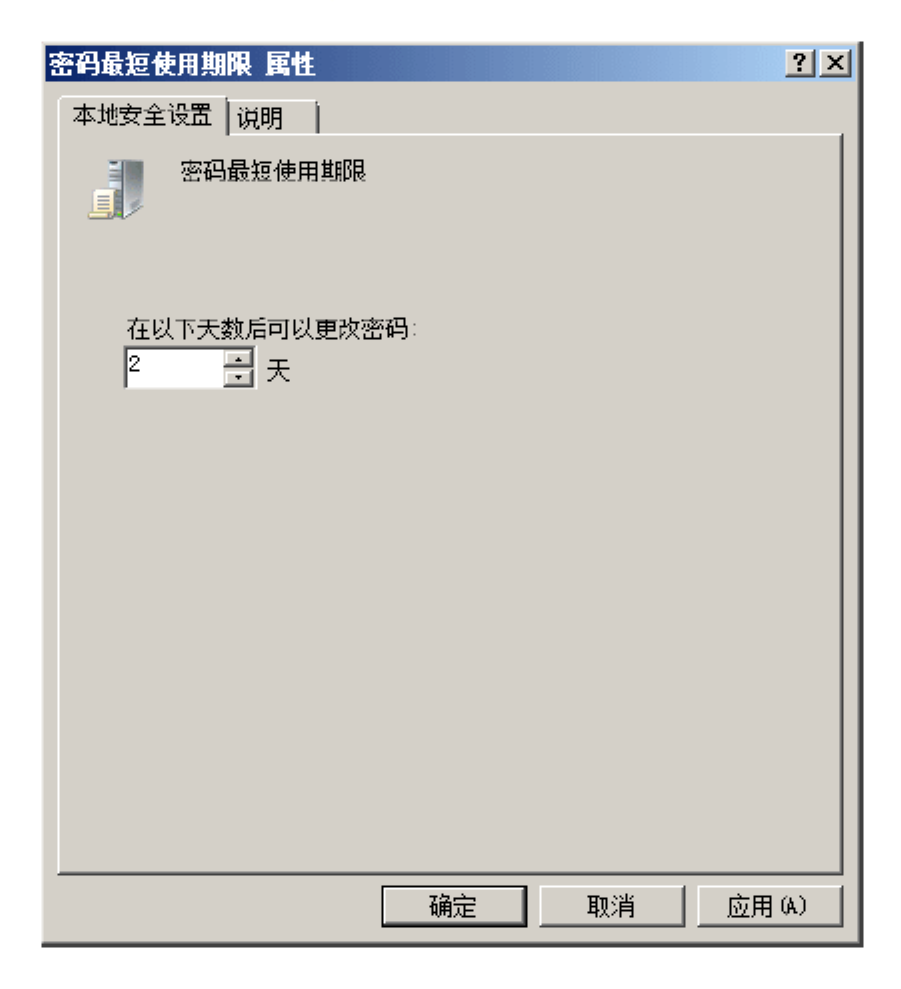


图 4-12　“密码最短使用期限 属性”对话框

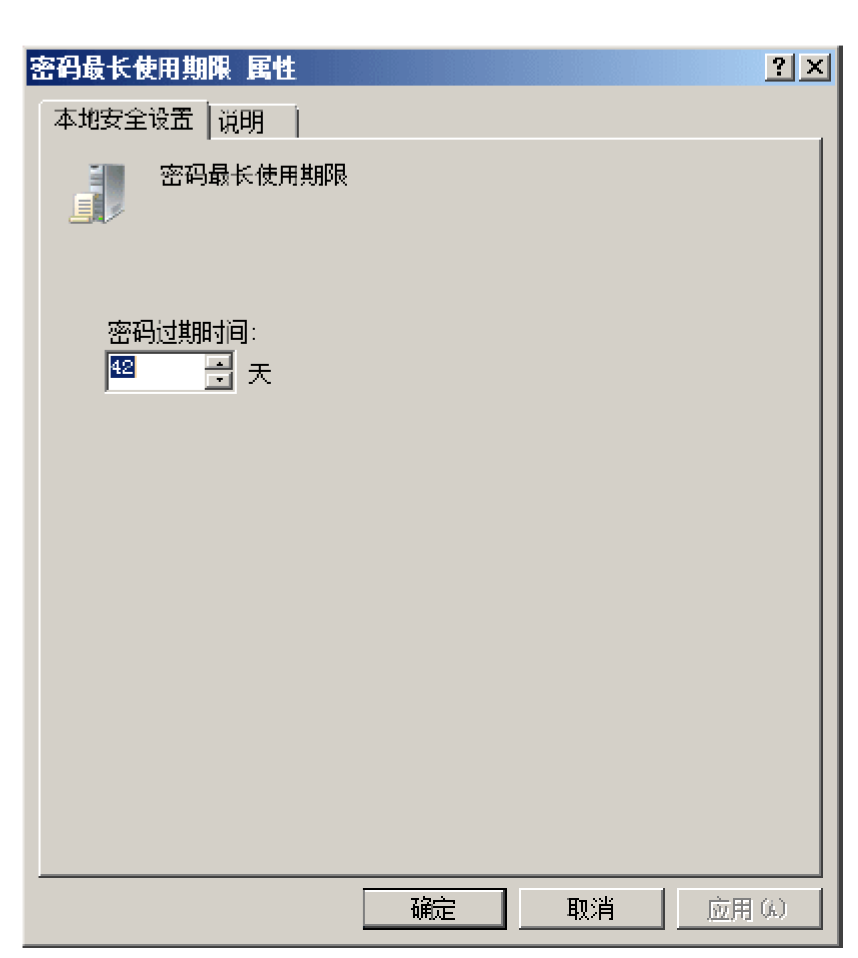


图 4-13　“密码最长使用期限 属性”对话框

注意：安全最佳操作是将密码设置为 30 到 90 天后过期，具体取决于系统环境及需求。这样，攻击者用来破解用户密码以及访问网络资源的时间将受到限制。

⑤ 双击“强制密码历史”策略，显示如图 4-14 所示的对话框，该策略用于限制用户更改账户密码之前不得使用的旧密码个数，有效范围为 0～24，例如，可以设置为 12，则用户不能重复使用在此之前用过的 12 个历史密码。在 Windows Server 2008 系统中，独立服务器上默认值为 0，域控制器上默认值为 24。

⑥ 双击“用可还原的加密来储存密码”策略，显示如图 4-15 所示对话框，该安全设置确定操作系统是否使用可还原的加密来储存密码。选择“已启用”单选按钮，表示允许使用可还原的加密存储密码。单击“确定”按钮保存设置。使用此安全设置，确定操作系统是否使用可还原的加密来储存密码，此策略还可以为某些应用程序提供支持。使用可还原的加密储存密码与储存纯文本密码，在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则绝不要启用此策略。

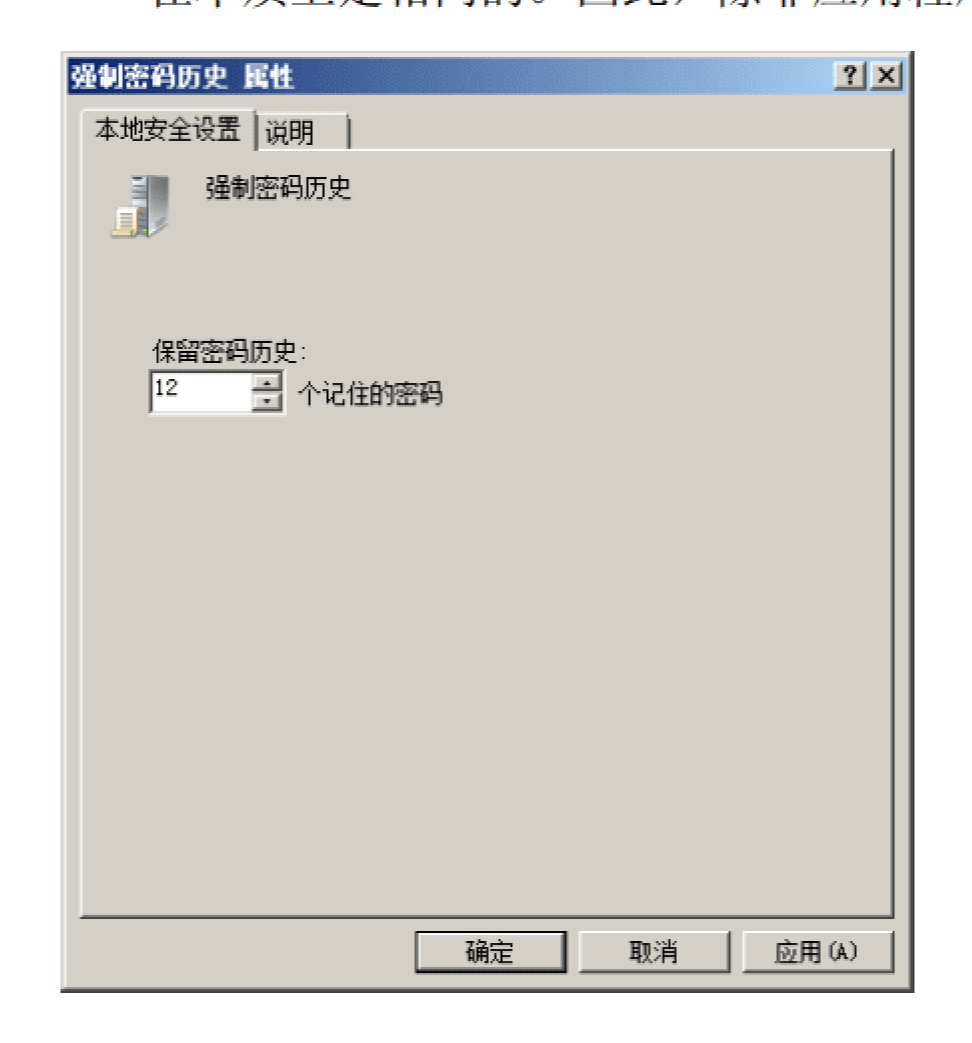


图 4-14 “强制密码历史 属性”对话框

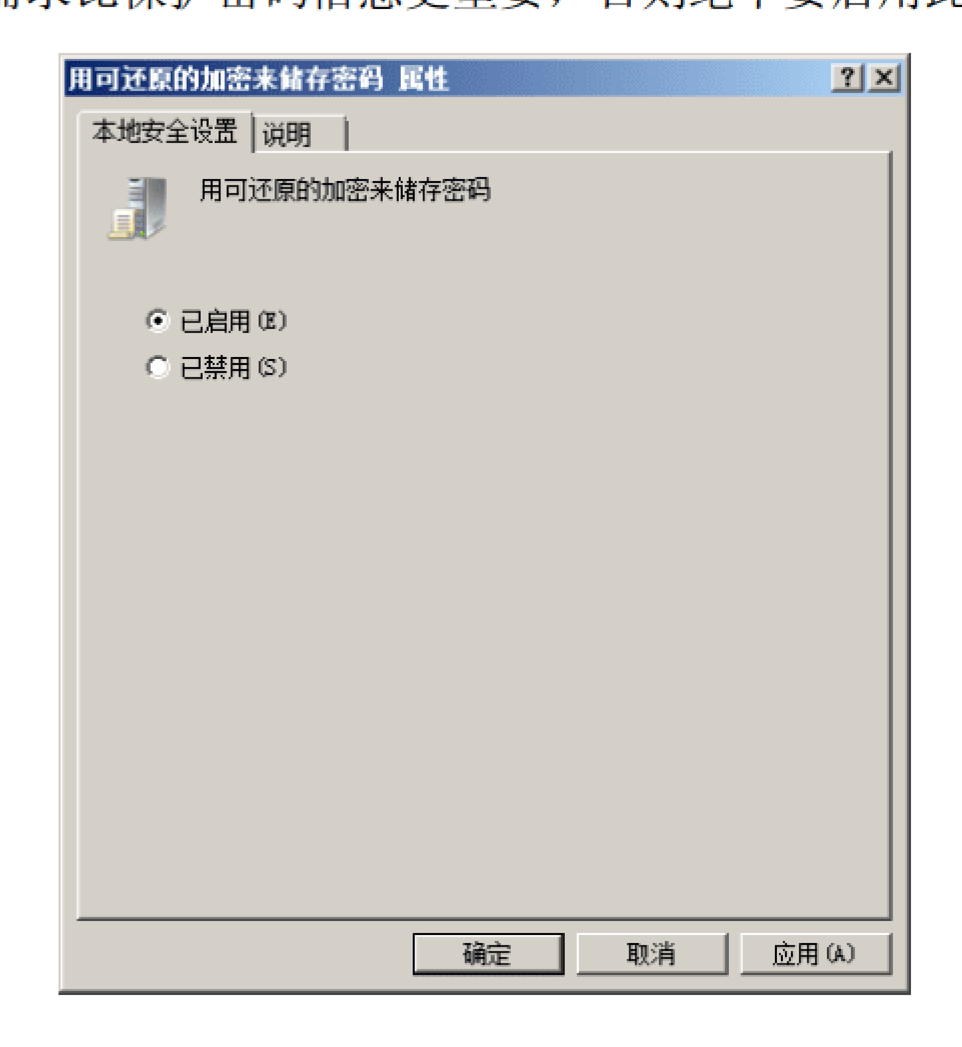


图 4-15 “用可还原的加密来储存密码 属性”对话框

2. 账户锁定策略

锁定账户可以有效防止入侵者无休止地尝试登录，账户锁定策略主要用于确定某个用户账户被锁定条件和时间长短，具体策略如下：

- 复位账户锁定计数器。
- 账户锁定时间。
- 账户锁定阈值。



提示：默认情况下，Windows Server 2008 系统的独立服务器并未配置“复位账户锁定计数器”策略和“账户锁定时间”策略，所以管理员账户无法对普通账户实施锁定。

① 在 Windows Server 2008 域控制器上，双击“复位账户锁定计数器”策略，显示如图 4-16 所示的对话框，选中“定义这个策略设置”复选框，并在“在此后复位账户锁定计数器”微调框中，输入适当的时间值，默认为 30 分钟，即账户被锁定 30 分钟后，方可再次尝试登录。如果定义了账

户锁定阈值，此重置时间必须小于或等于账户锁定时间。

② 在 Windows Server 2008 域控制器上，双击“账户锁定时间”策略，显示如图 4-17 所示的对话框，选中“定义这个策略设置”复选框，并在“账户锁定时间”微调框中，输入适当的时间值，默认锁定时间为 30 分钟。需要注意的是，只有在指定了账户锁定阈值时，此策略设置才有意义。

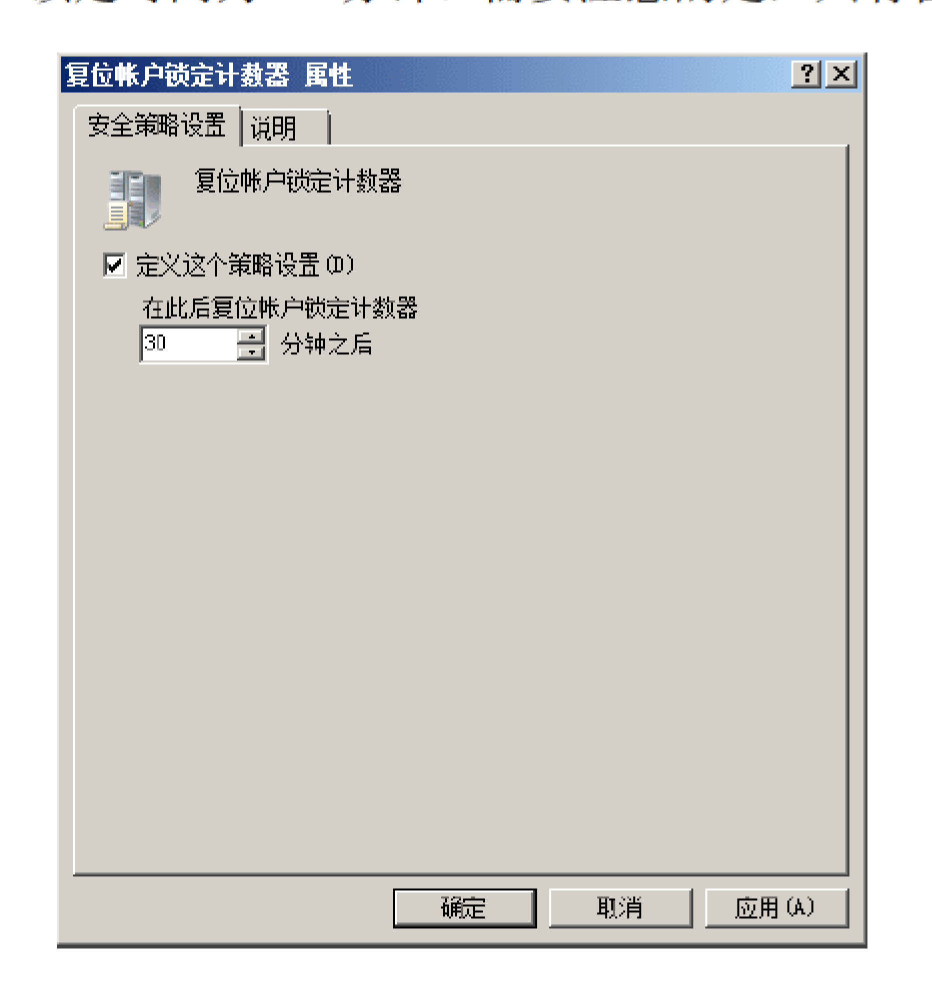


图 4-16　“复位账户锁定计数器 属性”对话框

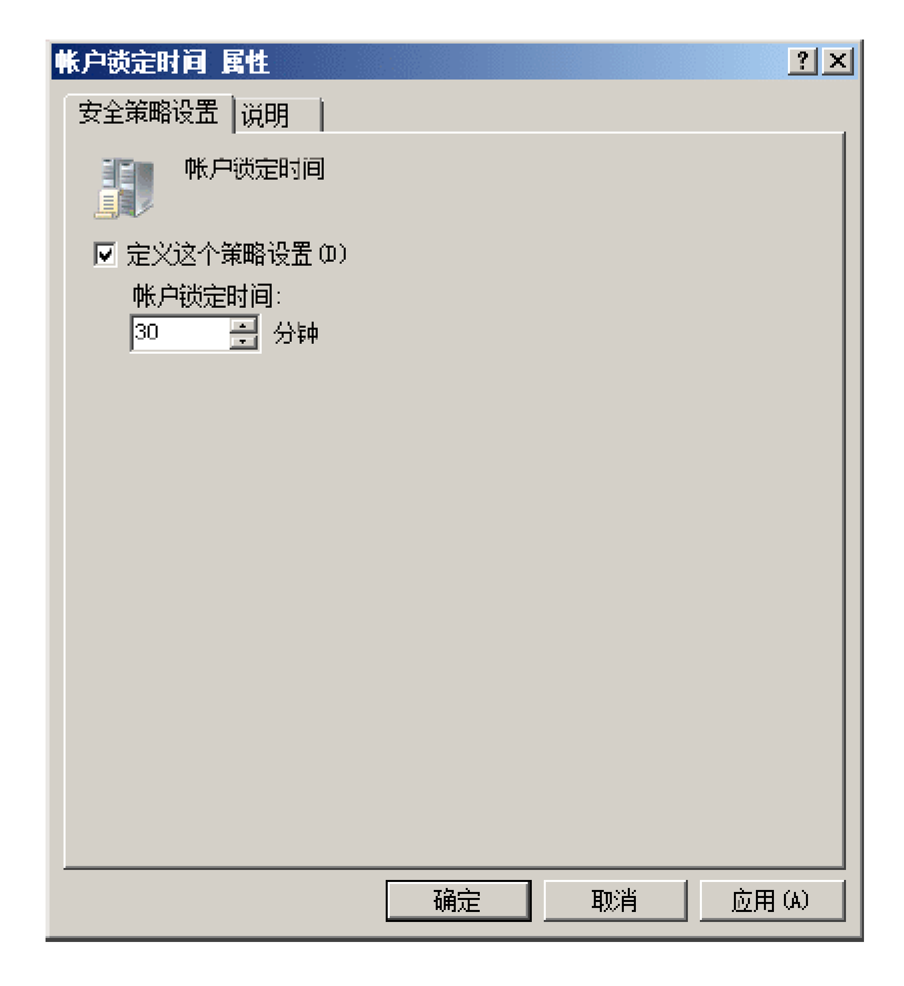


图 4-17　“账户锁定时间 属性”对话框

③ 在 Windows Server 2008 域控制器或独立服务器上，双击“账户锁定阈值”策略，显示如图 4-18 所示的对话框，选中“定义这个策略设置”复选框，即可启用该策略。Windows Server 2008 独立服务器的默认值为 0，即永不锁定账户，域控制器默认是未配置的。当使用 Ctrl+Alt+Del 或密码保护的屏幕保护程序锁定计算机时，也将记录失败尝试。

3. Kerberos 策略(Windows 域安全)

Kerberos 策略是适用于域用户账户的安全策略，独立服务器系统无此策略，主要用于确定与 Kerberos 相关的设置，例如票证的有效期限和强制执行。Kerberos 策略不存在于本地计算机策略中。Kerberos 策略中包含如下设置：

- 服务票证最长寿命。
- 计算机时钟同步的最大容差。
- 强制用户登录限制。
- 用户票证续订最长寿命。
- 用户票证最长寿命。

① 双击“服务票证最长寿命”，显示如图 4-19 所示的“服务票证最长寿命 属性”对话框，选中“定义这个策略设置”复选框，并在“票证过期时间”微调框中，设置适当值即可，默认为 600 分钟。该策略用来设置确定使用所授予的会话票证可访问特定服务的最长时间(以分钟为单位)。该设置必须大于 10 分钟，并且小于或等于用户票证最长寿命设置。

如果客户端请求服务器连接时出示的会话票证已过期，服务器将返回错误消息。客户端必须从 Kerberos V5 密钥分发中心(KDC)请求新的会话票证，然而一旦连接通过了身份验证，该会话票证是否仍然有效就无关紧要了。会话票证仅用于验证与服务器的新建连接。如果用于验证连接的会话票证在连接时过期，则当前的操作不会中断。

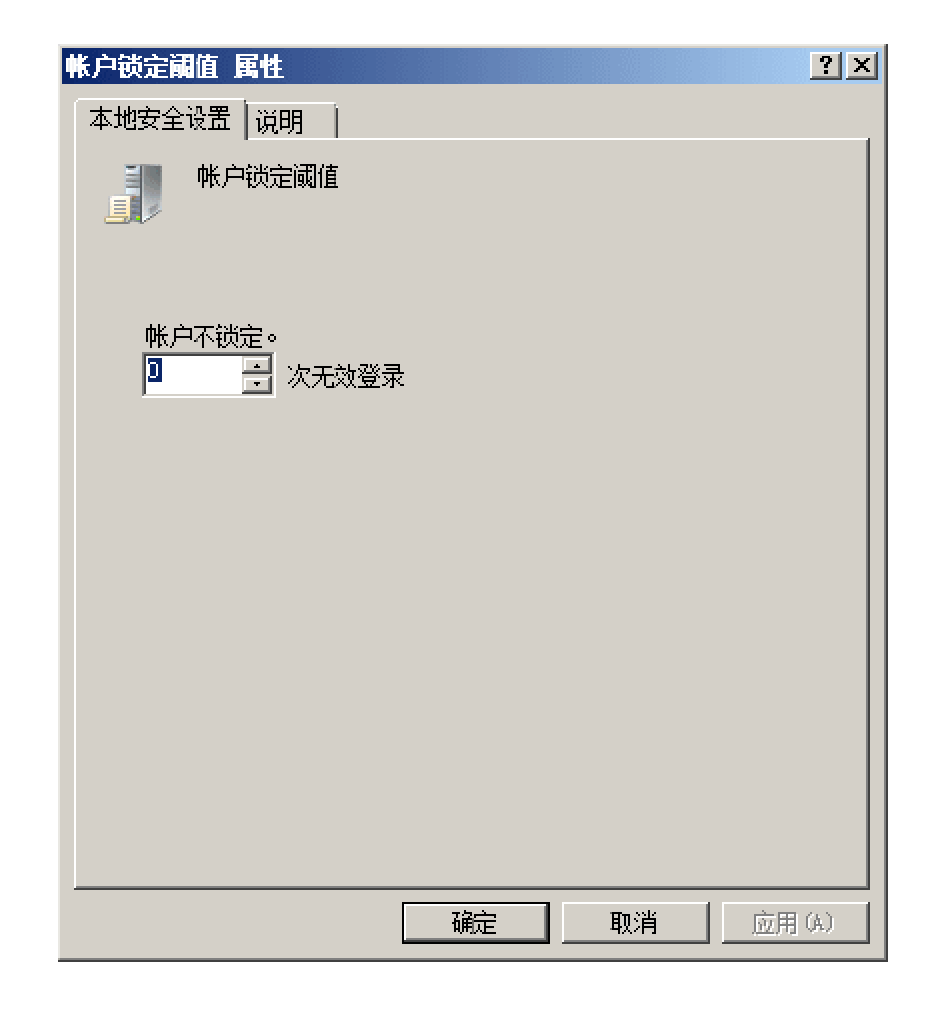


图 4-18 “账户锁定阈值 属性”对话框

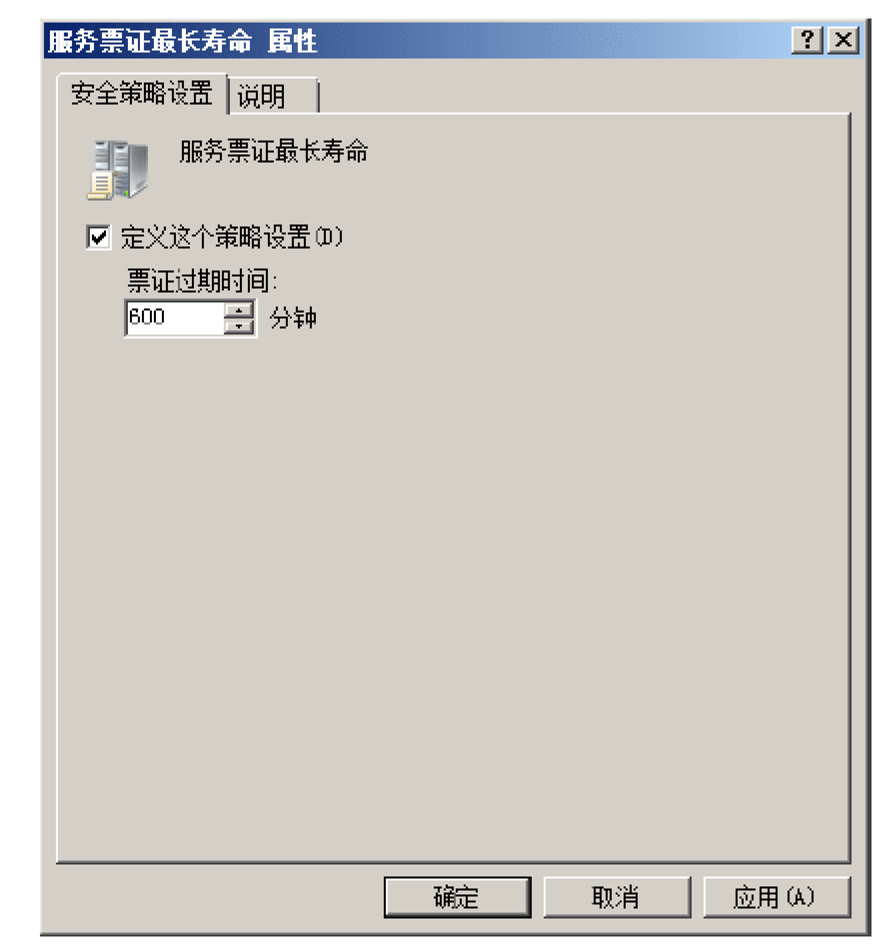


图 4-19 “服务票证最长寿命 属性”对话框

② 双击“计算机时钟同步的最大容差”策略，显示如图 4-20 所示的“计算机时钟同步的最大容差 属性”对话框，选中“定义这个策略设置”复选框，并在“最大容差”微调框中，设置适当值即可，默认为 5 分钟。该策略用来设置确定 Kerberos V5 所允许的客户端时钟和提供 Kerberos 身份验证的 Windows Server 2008 域控制器上的时间的最大差值。



提示：该设置并不是永久性的。如果配置该设置后重新启动计算机，那么该设置将被还原为默认值。

③ 双击“强制用户登录限制”策略，显示如图 4-21 所示的“强制用户登录限制 属性”对话框，选中“定义这个策略设置”复选框，并选择“已启用”单选按钮，即可启用该策略。该策略用来设置确定 Kerberos V5 密钥分发中心，是否要根据用户账户的用户权限验证每一个会话票证请求。验证每一个会话票证请求是可选的，因为额外的步骤需要花费时间，并可能降低服务的网络访问速度。

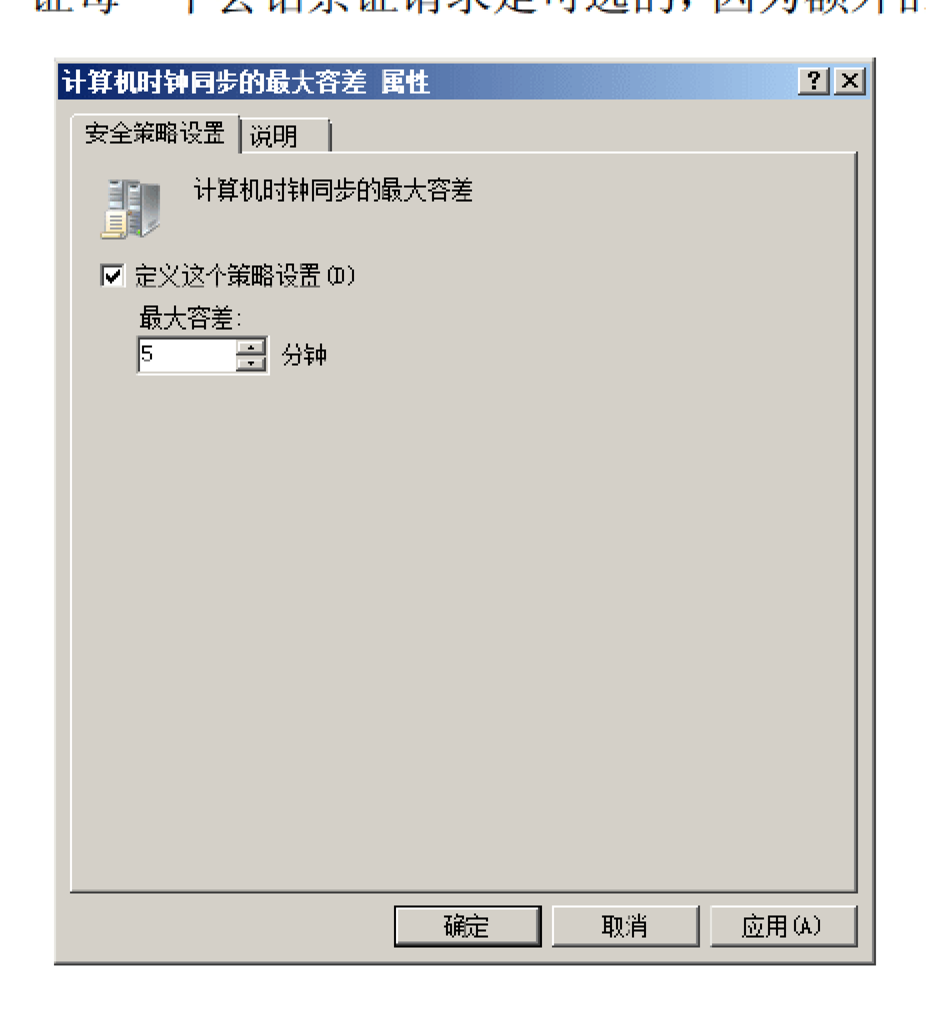


图 4-20 “计算机时钟同步的最大容差 属性”对话框

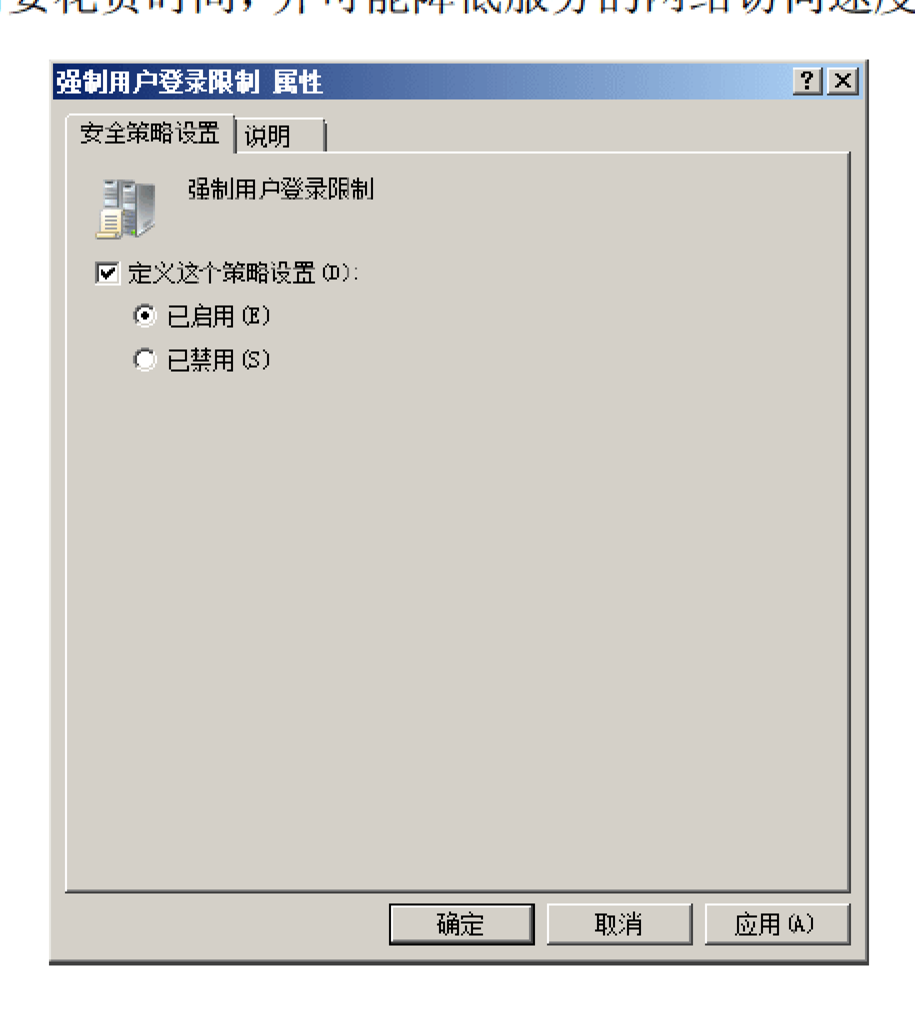


图 4-21 “强制用户登录限制 属性”对话框

④ 双击“用户票证续订最长寿命”策略，显示如图 4-22 所示的“用户票证续订最长寿命 属性”对话框，选中“定义这个策略设置”复选框，并在“票证续订过期时间”微调框中设置适当值即可，默认为 10 天。

⑤ 双击“用户票证最长寿命”策略，显示如图 4-23 所示的“用户票证最长寿命 属性”对话框，选中“定义这个策略设置”复选框，并在“票证过期时间”微调框中，设置适当值即可，默认为 7 小时。该策略用来设置确定用户票证授予票证(TGT)的最长使用时间，用户 TGT 期满后，必须请求新的或“续订”现有的用户票证。

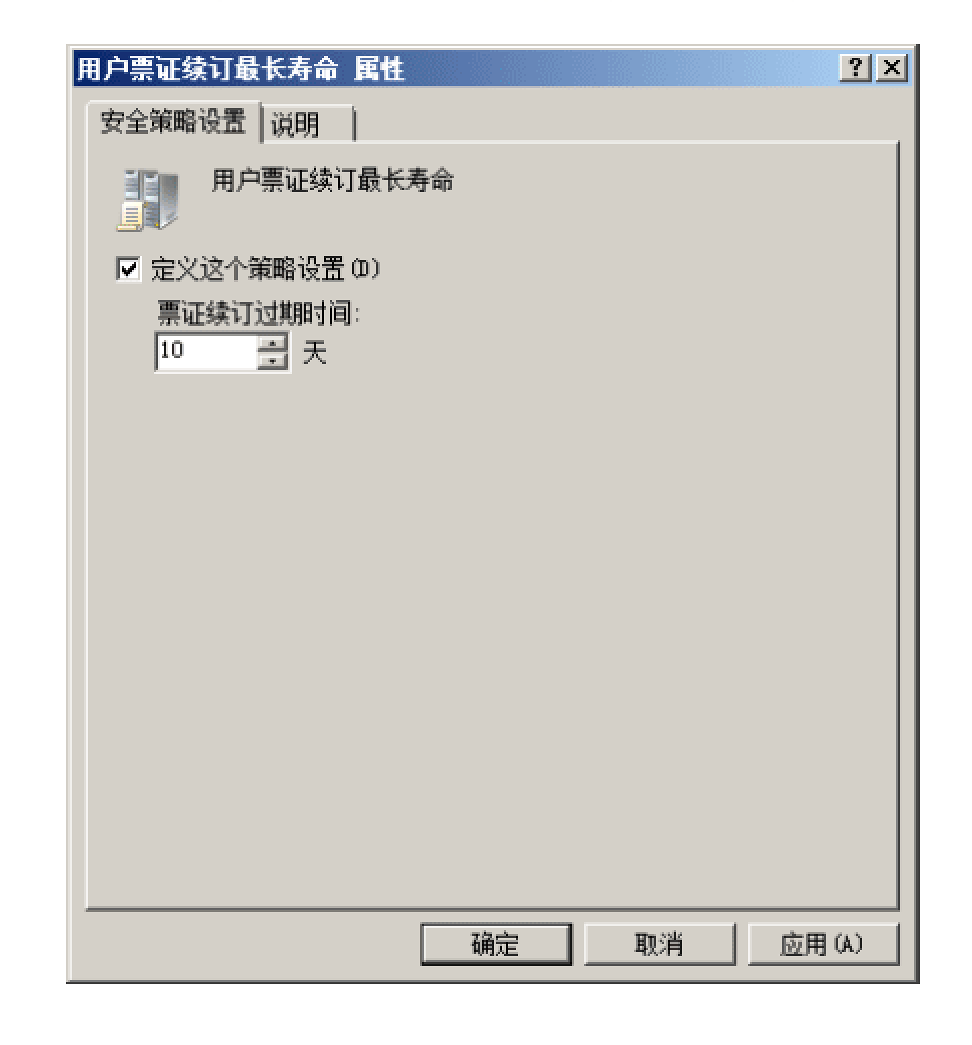


图 4-22 “用户票证续订最长寿命 属性”对话框

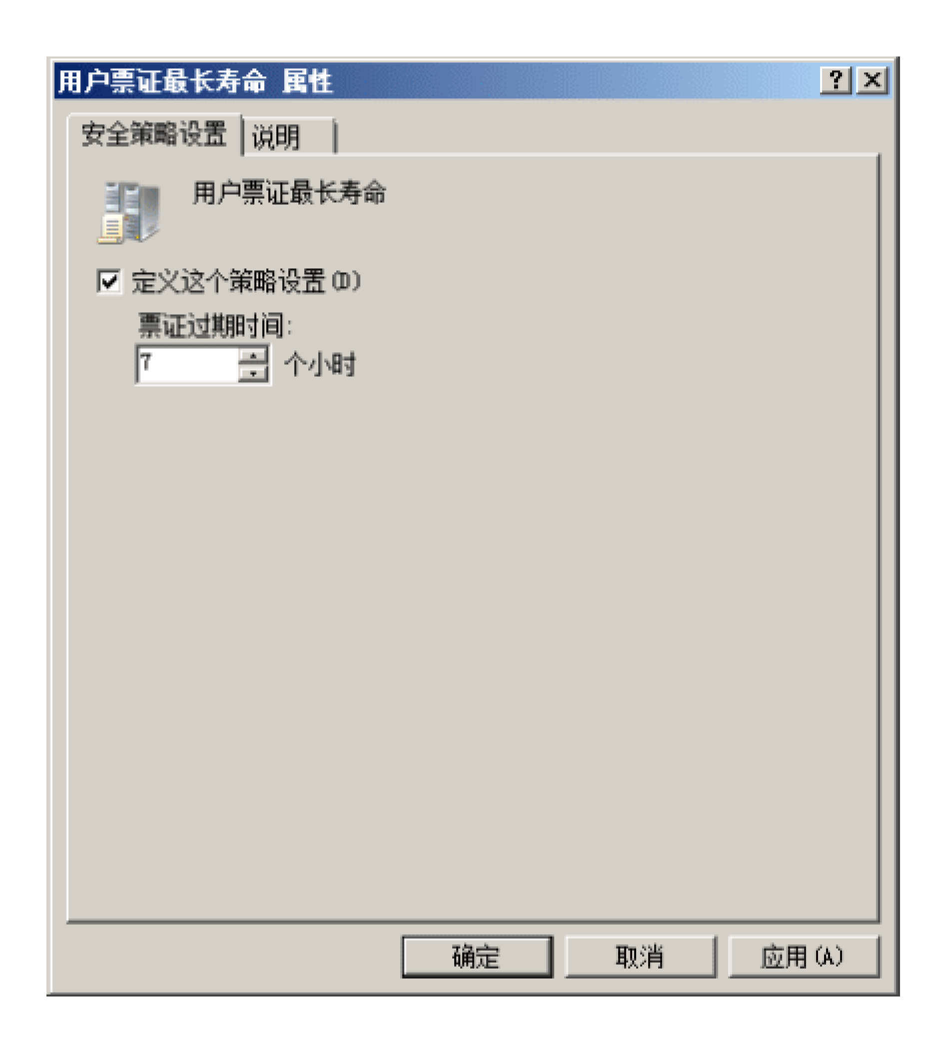


图 4-23 “用户票证最长寿命 属性”对话框

4. 推荐的密码策略设置

推荐的密码策略为：

- 密码必须符合复杂性要求：已启用，必须启用。
- 密码长度最小值：8 个字符或者更高。

推荐的账户锁定策略为：

- 账户锁定阀值：3 次(或者略高)无效登录。
- 账户锁定时间：30 分钟(默认，可根据实际需要更改)。
- 复位账户锁定计数器：30 分钟(默认，可根据实际需要更改)之后。



提示：密码复杂性是指密码中必须包含字母、数字、特殊符号等内容。对安全性要求比较高的地方，推荐使用超过 12 位以上的密码长度。密码应该经常性更换，特别在有管理员以外的人知道时。系统管理员 Administrator 密码建议仅有管理员知晓并且是足够强壮的密码，并且修改默认的用户名。

4.3.2 审核策略

审核是 Windows Server 2008 系统中本地安全策略的一部分，每当用户执行某些指定的操作时，审核日志都会记录一项。例如，对文件或策略进行修改就会触发审核项，以显示执行的操作、相关用户账户，

以及操作日期和时间。通过配置审核策略，系统可以自动记录所有登录到本地计算机的事件，因此，管理员只要在日志中发现在非工作时段或者陌生用户账户的系统登录，就能迅速判断系统被外来者入侵或试图入侵。各个审核设置的选项包括：

- 成功。请求的操作得以成功执行时会生成一个审核项。
- 失败。请求的操作失败时会生成一个审核项。
- 无审核。相关操作不会生成审核项。

通过审核可以记录下列 4 类信息：

- 哪些用户企图登录到系统中，或从系统中注销、登录或注销的日期和时间是否成功等。
- 哪些用户对指定的文件、文件夹或打印机进行哪种类型的访问。
- 系统的安全选项进行了哪些更改。
- 用户账户进行了哪些更改，是否增加或删除了用户等。

通过查看这些信息，系统管理员就能够及时发现系统存在的安全隐患，通过了解指定资源的使用情况来指定资源使用计划。Windows Server 2008 系统的审核策略包含以下 9 项：

- 审核策略更改。
- 审核登录事件。
- 审核对象访问。
- 审核过程跟踪。
- 审核目录服务访问。
- 审核特权使用。
- 审核系统事件。
- 审核账户登录事件。
- 审核账户管理。



提示： Windows 系列操作系统的日志审核默认为关闭状态，必须手动开启。审核策略设置完成后，需要重新启动计算机才能生效。

1. 配置审核策略

审核策略在本地计算机上打开“本地组策略编辑器”控制台，并依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”，显示如图 4-24 所示的“本地组策略编辑器”窗口，在右侧窗口中可以查看系统默认的所有策略。

Windows Server 2008 系统审核策略的主要功能如表 4-1 所示。

表 4-1　审核策略及功能说明

审核策略	功能说明
审核策略更改	该安全设置确定是否审核用户权限分配策略、审核策略或信任策略更改的每一个事件
审核登录事件	该安全设置确定是否审核每一个登录或注销计算机的用户账户。在域控制器上，将生成域账户活动的账户登录事件，并在本地计算机上生成本地账户活动的账户登录事件
审核对象访问	该安全设置确定是否审核用户访问某个对象的事件，例如文件、文件夹、打印机等，都有自己特定的系统访问控制列表(SACL)

续表

审核策略	功能说明
审核过程跟踪	该安全设置确定是否审核事件的详细跟踪信息，例如进程的启动和退出等
审核目录服务访问	该安全设置确定是否审核用户访问那些指定自己的系统访问控制列表的 Active Directory 对象的事件。默认情况下，在“默认域控制器组策略对象(GPO)”中该值设置为无审核，并且在该值没有任何意义的工作站和服务器中，它保持未定义状态
审核特权使用	该安全设置确定是否审核用户实施其用户权利的每一个事件
审核系统事件	当用户重新启动或关闭计算机时或者对系统安全或安全日志有影响的事件发生时，安全设置确定是否予以审核
审核账户登录事件	该安全设置确定是否审核在这台计算机用于验证账户时，用户登录到其他计算机或者从其他计算机注销的每个实例。当在域控制器上对域用户账户进行身份验证时，将产生账户登录事件。该事件记录在域控制器的安全日志中。当在本地计算机上对本地用户进行身份验证时，将产生登录事件。该事件记录在本地安全日志中。不产生账户注销事件
审核账户管理	该安全设置确定是否审核计算机上的每一个账户管理事件

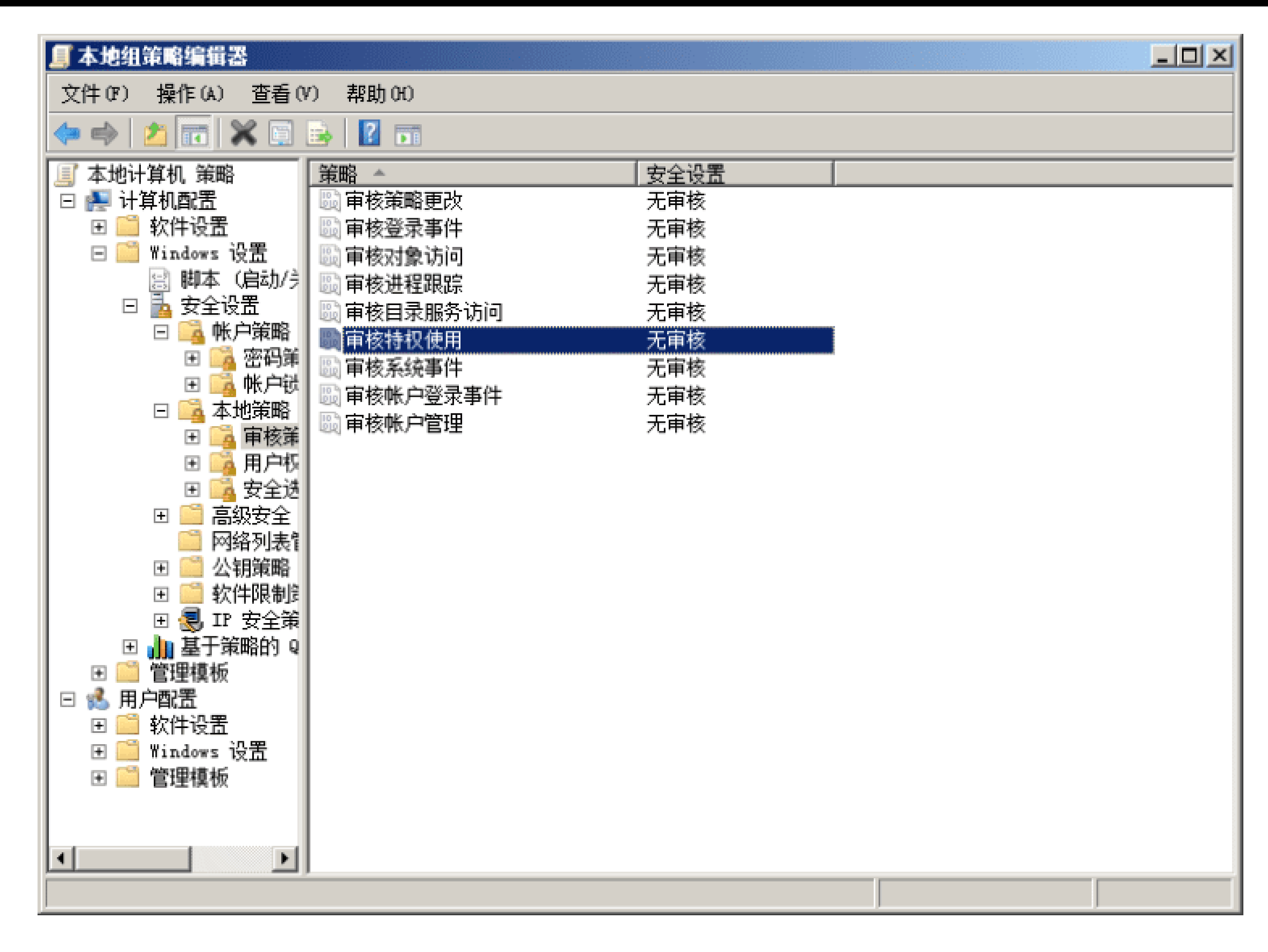


图 4-24　“本地组策略编辑器”窗口

此处以配置“审核策略更改”策略为例，介绍 Windows Server 2008 本地计算机审核策略的配置。

① 在“审核策略”窗口中，双击“审核策略更改”策略，显示如图 4-25 所示的“审核策略更改 属性”对话框。同时选中“成功”和“失败”复选框，系统即可同时记录所有“成功”和“失败”的策略更改事件。在域控制器上该策略默认为只审核“成功”的操作，在独立服务器上默认设置为“无审核”，即不记录任何此类事件。

② 单击“说明”标签切换至如图 4-26 所示的“说明”选项卡，可以查看该策略的说明信息。

③ 单击“确定”按钮，保存设置即可。配置其他审核策略的操作步骤与此完全相同，不再赘述。

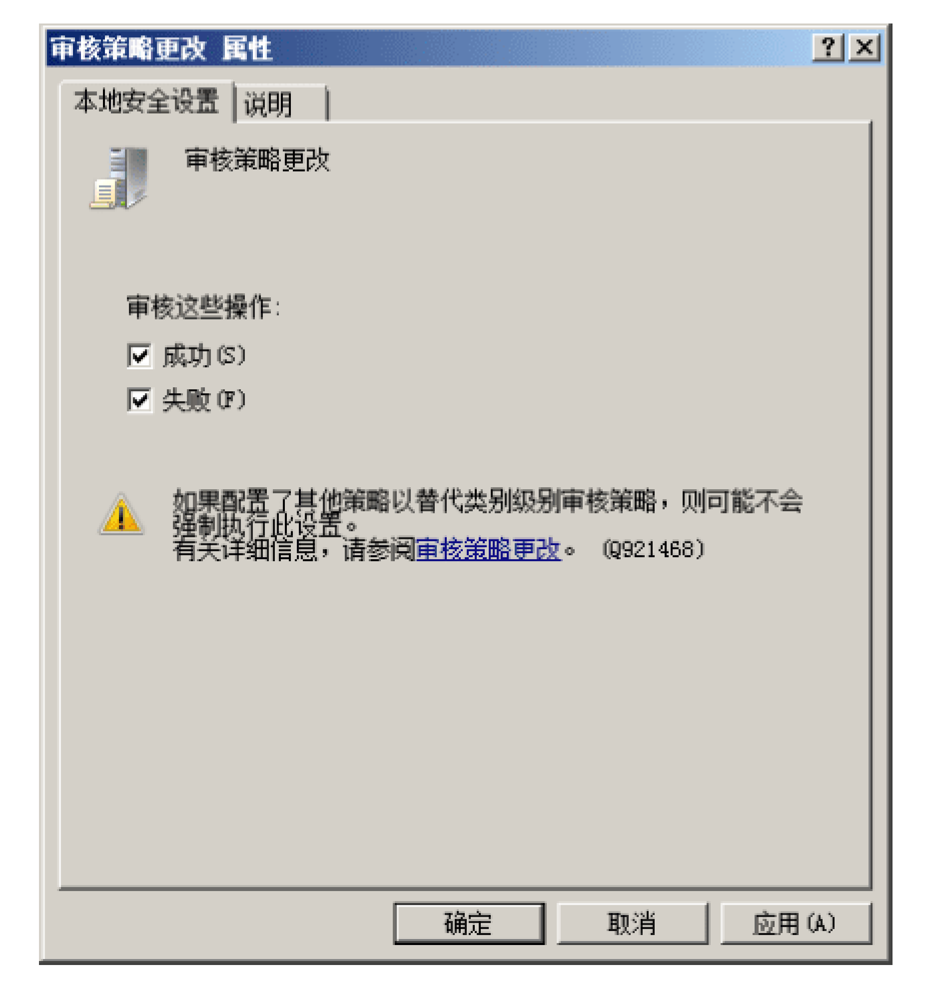


图 4-25 “审核策略更改 属性”对话框

图 4-26 策略说明信息

2. 推荐的审核策略设置

推荐的审核策略配置目标有以下内容。

- 审核策略更改：成功+失败。
- 审核登录事件：成功+失败。
- 审核访问对象：失败。
- 审核目录服务访问：失败。
- 审核特权使用：失败。
- 审核系统事件：成功+失败。
- 审核账户登录事件：成功+失败。
- 审核账户管理：成功+失败。

3. 调整日志审核文件的大小

配置和启用审核策略后，系统将自动对指定事件进行审核和记录，默认情况下这些事件记录保存在Windows 事件查看器指定的目录(%SystemRoot%\System32\Winevt\Logs\)下。在安装 Windows Server 2008 系统时，默认已经设置了日志文件大小，除“安装程序”日志为 1024KB 外，“应用程序”、“安全”、“系统”和“转发的事件”日志大小上限均为 20MB。对于网络服务器而言，建议适当增大日志文件大小的上限值。推荐的日志空间大小为：

- 应用程序日志，51200KB，即 50MB。
- 安全日志，1024000KB，即 1000MB。
- 系统日志，102400KB，即 100MB。

这里以“安全”日志审核文件为例，介绍如何调整 Windows 日志文件存储空间上限值。

① 依次选择“开始”→“管理工具”→“事件查看器”，显示如图 4-27 所示的“事件查看器”窗口。

② 右击“安全”并选择快捷菜单中的“属性”选项，显示如图 4-28 所示的“日志属性 – 安全”对话框。在“日志最大大小”微调框中输入“1024000”，即 1000MB，并选择“日志满时将其存

档，不覆盖事件”单选按钮，以免丢失旧的事件日志。

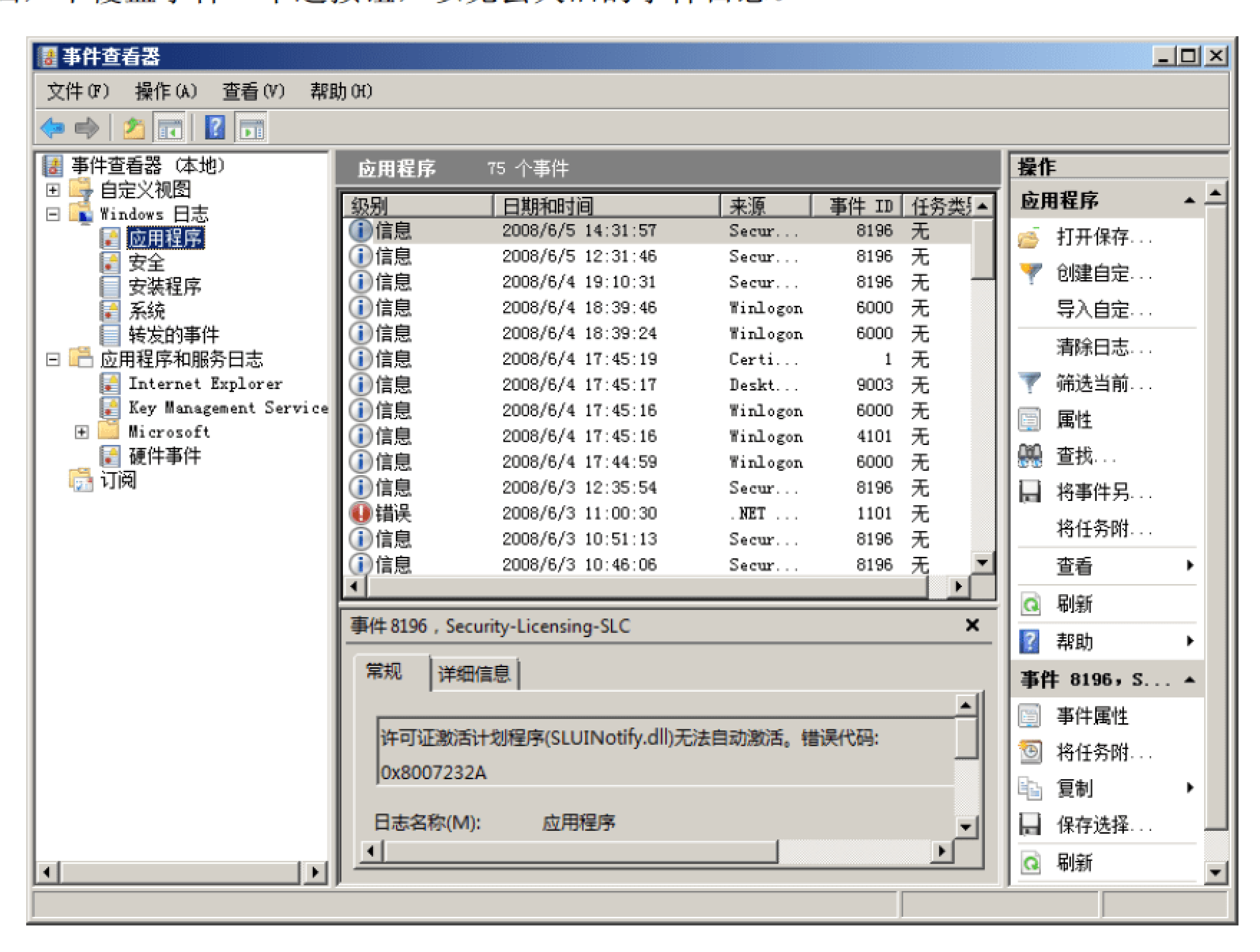


图 4-27　“事件查看器”窗口

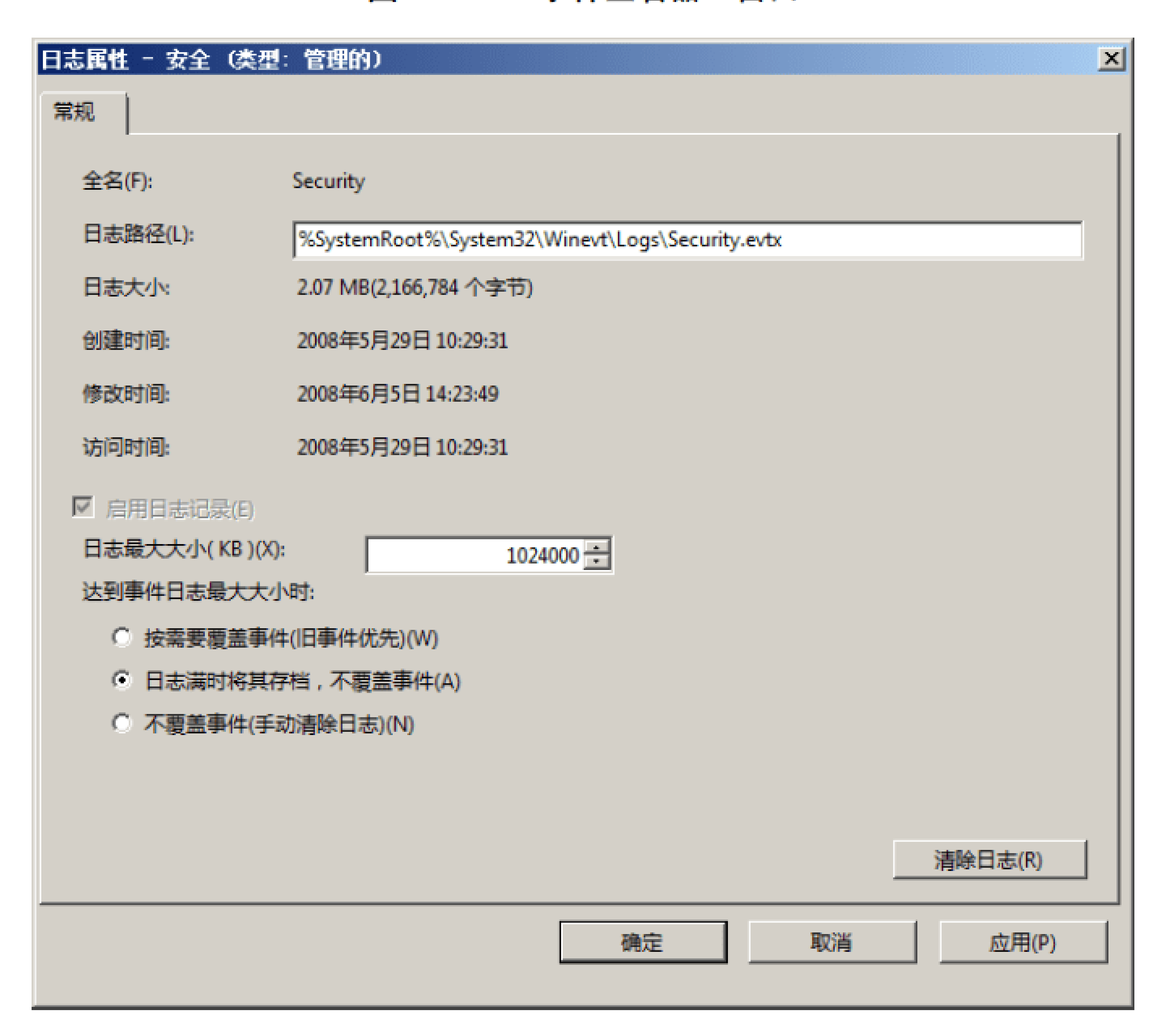
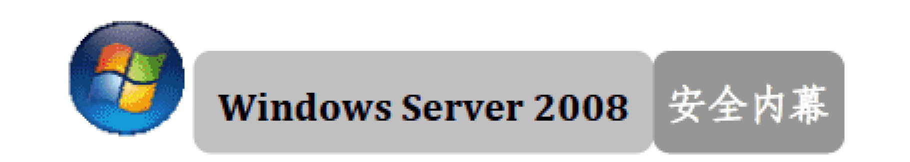


图 4-28　“日志属性 – 安全”对话框

③ 单击“确定”按钮，即可完成日志文件大小的修改。使用相同的方法即可更改其他类型日志审核文件大小的最大值。




注意：日志文件的大小必须是 64K 的倍数。

4.3.3　用户权限分配

将部分安全功能设置权限，分配给特定的用户账户，既可以减少系统或网络管理员的工作负担，又可以做到重要权限的分散，避免了个别用户权限过高而给系统或网络带来的威胁。在“本地组策略编辑器”窗口中，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”选项，即可查看 Windows Server 2008 系统中的用户权限分配策略，如图 4-29 所示。

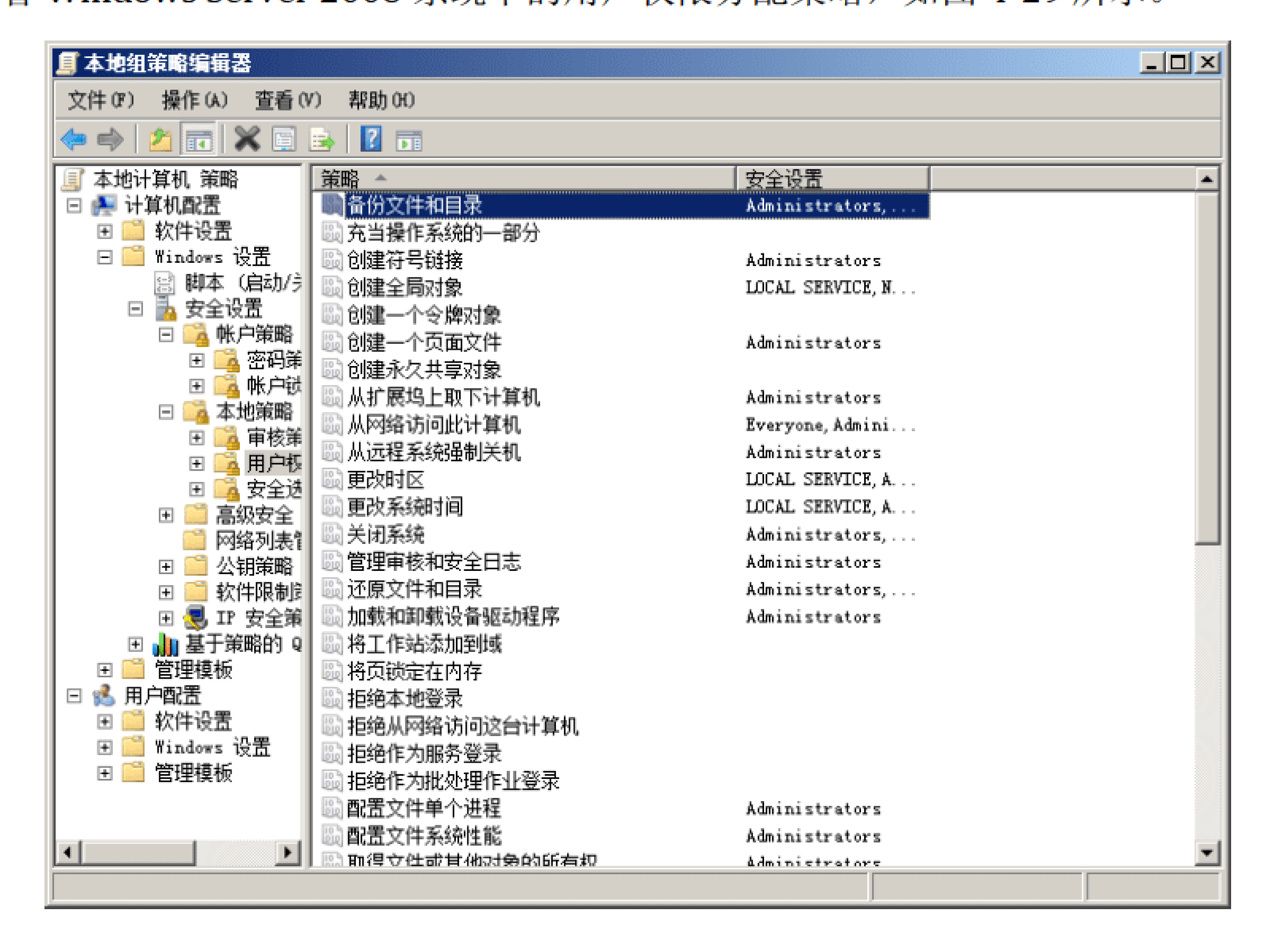


图 4-29　用户权限分配策略

在 Windows Server 2008 系统中，管理员可以为用户账户指派更为详细的安全管理权限，可分配权限及功能描述如表 4-2 所示。

表 4-2　用户权限分配策略及功能

策　略	功能说明	默认用户账户和组
备份文件和目录	确定哪些用户可以绕过文件和目录、注册表和其他永久对象权限进行系统备份	Administrators 、 Backup Operators
充当操作系统的一部分	此用户权限允许某个进程模拟任意用户而无须进行身份验证。因此该进程可以与该用户一样获得对本地资源的访问权限	
创建符号链接	此权限决定用户是否可以从登录的计算机创建符号链接	Administrators
创建全局对象	此用户权限对于在终端服务会话过程中创建全局对象的用户账户是必需的。未分配此用户权限的用户仍可以创建特定于会话的对象	Local Service 、 Network Service、Administrators、Service

续表

策　略	功能说明	默认用户账户和组
创建一个令牌对象	此安全设置确定进程可以使用哪些账户创建令牌，该令牌接着可以在进程使用内部应用程序编程接口(API，Application Programming Interface)创建访问令牌时用于获取任何本地资源的访问权限。此用户权限供操作系统内部使用。除非必要，建议不要将此用户权限分配给本地系统之外的用户、组或进程	没有任何用户账户。
创建一个页面文件	此用户权限确定哪些用户和组可以调用内部应用程序编程接口(API)创建页面文件。此用户权限供操作系统内部使用，且通常不需要分配给任何用户	Administrators
创建永久共享对象	此用户权限确定进程可以使用哪些账户利用对象管理器创建目录对象。此用户权限供操作系统内部使用，且对于扩展对象命名空间的内核模式组件非常有用	没有任何用户账户。
从扩展坞上取下计算机	此安全设置确定用户是否可以无需登录而从其扩展坞上移除便携式计算机	Administrators
从网络访问此计算机	此用户权限确定允许哪些用户和组通过网络连接到计算机。此用户权限不影响终端服务	Everyone、Administrators、Users、Backup Operators
从远程系统强制关机	此安全设置确定允许哪些用户从网络上的远程位置关闭计算机。误用此用户权限会导致拒绝服务。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	Administrators
更改时区	此用户权限确定哪些用户和组可以更改计算机默认时区。这是 Windows Server 2008 的新增用户权限分配策略之一	Local Service、Administrators
更改系统时间	此用户权限确定哪些用户和组可以更改计算机内部时钟上的日期和时间。分配了此用户权限的用户可以影响事件日志的外观。如果已更改了系统时间，则记录的事件将反映此新时间，而不是事件发生的实际时间	Local Service、Administrators
关闭系统	此安全设置确定哪些在本地登录到计算机的用户可以使用关机命令关闭操作系统。误用此用户权限会导致拒绝服务	Administrators 、 Backup Operators
管理审核和安全日志	此安全设置确定哪些用户可以为单独的资源(如文件、Active Directory 对象和注册表项)指定对象访问审核选项	Administrators
还原文件和目录	此安全设置确定在还原备份的文件和目录时哪些用户可以绕过文件、目录、注册表和其他永久对象权限，以及确定哪些用户可以将任何有效的安全主体设置为对象的所有者	Administrators 、 Backup Operators
加载和卸载设备驱动程序	此用户权限确定哪些用户可以将设备驱动程序或其他代码动态加载和卸载到内核模式中。此用户权限不适用于即插即用设备驱动程序。建议不要将此权限分配给其他用户	Administrators
将工作站添加到域	此安全设置确定哪些组或用户可以将工作站添加到域。此安全设置仅对域控制器有效。默认情况下，任何已经经过身份验证的用户都具有此权限并可以在该域中最多创建 10 个计算机账户	没有任何用户账户

续表

策　略	功能说明	默认用户账户和组
将页锁定在内存	此安全设置确定哪些账户可以使用进程将数据保持在物理内存中，这样可防止系统将数据分页到磁盘上的虚拟内存中。使用此权限会因降低可用随机存取内存(RAM)的数量，而显著影响系统性能	没有任何用户账户。
拒绝本地登录	此安全设置确定要防止哪些用户在该计算机上登录。如果账户受制于此策略设置和“允许本地登录”策略设置，则前者会取代后者	没有任何用户账户。
拒绝从网络访问这台计算机	此安全设置确定要防止哪些用户通过网络访问计算机。如果用户账户受限于此策略设置和“从网络访问此计算机”策略设置，则前者会取代后者	没有任何用户账户。
拒绝作为服务登录	此安全设置确定要防止哪些服务账户将进程注册为服务。如果账户受制于此策略设置和“作为服务登录”策略设置，则前者会取代后者	没有任何用户账户。
拒绝作为批处理作业登录	此安全设置确定要防止哪些账户作为批处理作业登录。如果用户账户受限于此策略设置和“作为批处理作业登录”策略设置，则前者会取代后者	没有任何用户账户。
配置文件单个进程	此安全设置确定哪些用户可以使用性能监视工具来监视非系统进程的性能	Administrators
配置文件系统性能	此安全设置确定哪些用户可以使用性能监视工具来监视系统进程的性能	Administrators
取得文件或其他对象的所有权	此安全设置确定哪些用户可以取得系统中任何安全对象(包括 Active Directory 对象、文件和文件夹、打印机、注册表项、进程以及线程)的所有权	Administrators
绕过遍历检查	此用户权限确定哪些用户即使在不具有对已遍历目录的权限时，也可以遍历目录树。此权限不允许用户列出目录的内容，仅允许遍历目录。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	Everyone、Local Service、Network Service、Administrators、Users、Backup Operators
身份验证后模拟客户端	将此权限分配给用户使代表该用户运行的程序能够模拟客户端。此种模拟要求此用户权限可防止未经授权的用户说服客户端连接(例如，通过远程过程调用(RPC)或命名管道)到他们已创建的服务，然后模拟该客户端，这样会将未经授权的用户的权限提升至管理级别或系统级别	Local Service、Network Service、Administrators、Service
生成安全审核	此安全设置确定进程可以使用哪些账户将项目添加到安全日志中。安全日志用于跟踪未授权的系统访问。如果启用了“审核：如果无法记录安全审核，则立即关闭系统”安全策略设置，则误用此用户权限会导致生成许多审核事件，可能隐藏攻击证据或导致拒绝服务	Local Service、Network Service
提高计划优先级	此安全设置确定哪些账户可以使用对另一个进程具有 Write Property 访问权限的进程来提高分配给其他进程的执行优先级。具有此权限的用户可以通过任务管理器用户界面更改进程的计划优先级	Administrators
替换一个进程级令牌	此安全设置确定哪些用户账户可以调用应用程序编程接口，从而使一个服务能够启动另一个服务。任务计划程序是使用此用户权限的进程的一个示例。有关任务计划程序的信息，请参阅任务计划程序概述	Local Service、Network Service

续表

策　略	功能说明	默认用户账户和组
调试程序	此用户权限确定哪些用户可以将调试程序连接到任何进程或连接到内核。不需要将此用户权限分配给正在调试自己的应用程序的开发人员。调试新系统组件的开发人员将需要此用户权限来执行相应操作。此用户权限提供对敏感和关键系统组件的完全访问权限	Administrators
通过终端服务拒绝登录	此安全设置确定禁止哪些用户和组作为终端服务客户端登录	没有任何用户账户
通过终端服务允许登录	此安全设置确定哪些用户或组具有作为终端服务客户端登录的权限	Administrators、Remote Desktop Users
同步目录服务数据	此安全设置确定哪些用户和组有权同步所有目录服务数据，也称为 Active Directory 同步	没有任何用户账户。
为进程调整内存配额	此权限确定谁可以更改进程可消耗的最大内存。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	Local Service、Network Service、Administrators
信任计算机和用户账户可以执行委派	此安全设置确定哪些用户可以在用户或计算机对象上，设置“已为委派信任”设置	没有任何用户账户
修改固件环境值	此安全设置确定谁可以修改固件环境值。固件环境变量是在非基于 x86 的计算机的稳定 RAM 中存储的设置。该设置的效果依赖于处理器	Administrators
修改一个对象标签	此权限决定哪些用户账户可以修改对象(例如文件、注册表项或其他用户所拥有的进程)的完整性标签。在用户账户下运行的进程可以将该用户所拥有的对象标签修改为没有此权限的更低级别	没有任何用户账户
允许在本地登录	此登录权限确定哪些用户能以交互方式登录到此计算机。通过在连接的键盘上按 Ctrl+Alt+Del 组合键序列启动的登录要求用户具有此登录权限。此外，可以登录用户的某些服务或管理应用程序可能要求此登录权限。如果为某个用户或组定义此策略，则还必须向 Administrators 组授予此权限	Administrators、Users、Backup Operators
增加进程工作集	此安全设置确定允许那些用户增加运行进程时所需访问的页面数量	Users
执行卷维护任务	此安全设置确定哪些用户和组可以在卷上运行维护任务，如远程碎片整理。需要注意的是，具有此用户权限的账户可以浏览磁盘及将文件扩展到包含其他数据的内存中。当打开扩展的文件时，用户可能能够读取和修改获得的数据	Administrators
作为服务登录	此安全设置确定哪些服务账户可以将进程注册为服务	没有任何用户账户
作为批处理作业登录	此安全设置使用户能够通过批处理队列实用程序登录，并仅提供用于与旧版本的 Windows 的兼容性	Administrators、Backup Operators、Performance Log Users
作为受信任的呼叫方访问凭据管理器	此安全设置用于确定哪些远程访问账户可以访问本地服务器或网络上的凭据管理器，存在很大的风险，建议不要轻易使用	没有任何用户账户

这里以“备份文件和目录”为例，介绍如何配置用户权限分配策略。主要操作步骤如下。

① 双击“备份文件和目录”策略，显示如图 4-30 所示的“备份文件和目录 属性”对话框，列表中显示的是策略默认的用户账户和组。

② 单击“添加用户或组”按钮，显示如图 4-31 所示的“选择用户或组”对话框。在“输入对象名称来选择”文本框中，输入想要添加的用户账户或组。

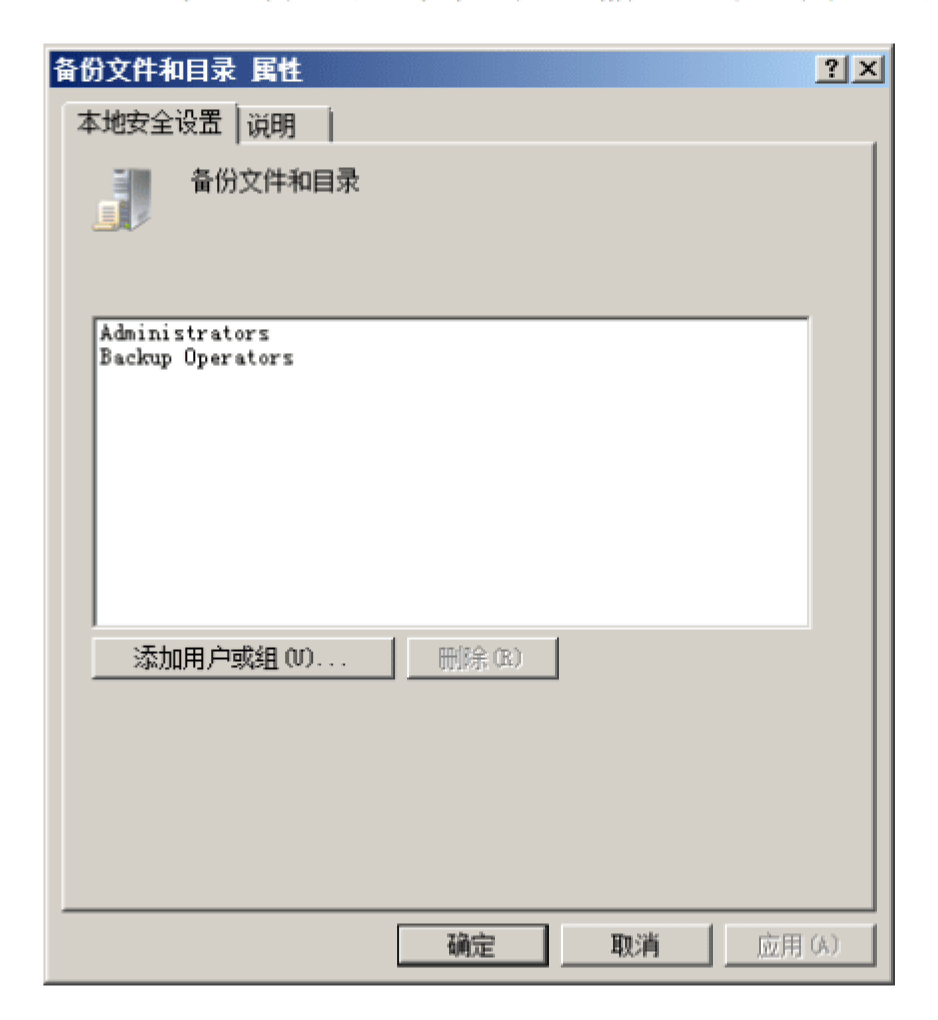


图 4-30 “备份文件和目录 属性”对话框



图 4-31 “选择用户或组”对话框

③ 单击“确定”按钮，即可将其添加至策略允许的对象列表中，如图 4-32 所示。

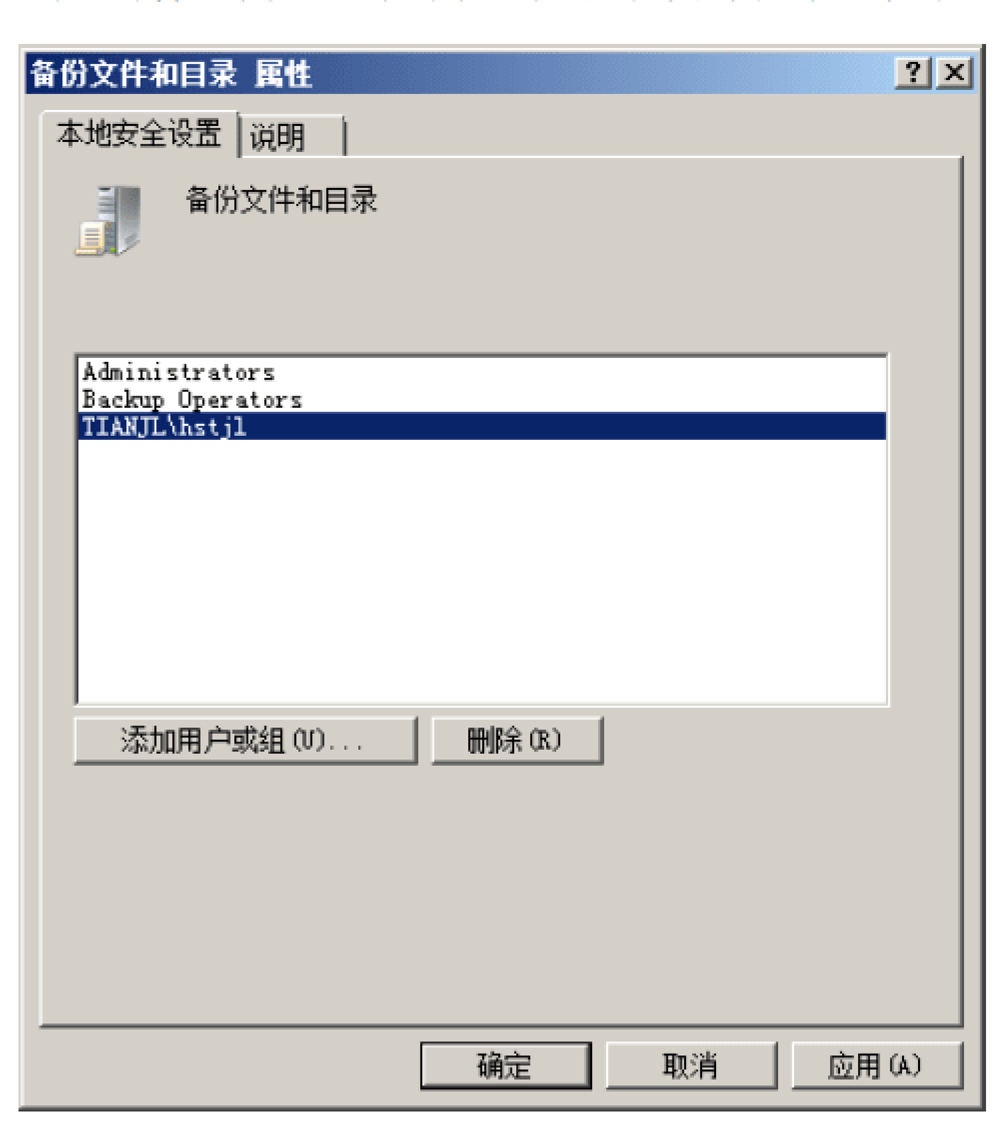


图 4-32 成功为策略允许的对象列表添加用户账户

④ 单击“确定”按钮，保存设置即可。使用相同的方法即可定义其他用户权限分配策略，此处不复赘述。

4.3.4　设备限制安全策略

通过在所有客户端计算机上部署硬件设备安装限制安全策略，可以阻止用户随便在计算机上安装任何硬件设备，导致不必要的系统安全问题。例如，通过限制使用 U 盘等可移动存储设备，不仅可以阻止部分病毒的传播，还可以避免重要的信息失窃。组策略中的管理模板策略有两个级别的控制权，第一个级别可以阻止设备驱动的安装，特别是移动存储设备。第二个级别控制对资源的访问。管理员通过限制从可移动存储设备中读取和向其中写入的数据，就可以保护内部数据安全。



提示：此处以硬件设备的 GUID 为例，禁止安装指定的硬件设备。

① 将任意 U 盘插入计算机的 USB 接口，打开“计算机管理”→“设备管理器”窗口，展开“磁盘驱动器”选项，显示如图 4-33 所示的窗口。

② 右击 U 盘对应的设备名称，选择“属性”选项，在打开对话框中单击“详细信息”，切换至如图 4-34 所示的“详细信息”选项卡。在“属性”下拉列表框中选择“设备类 GUID”选项，在“值”列表框中显示的就是 U 盘类设备对应的 GUID，将此值复制到粘贴板即可。

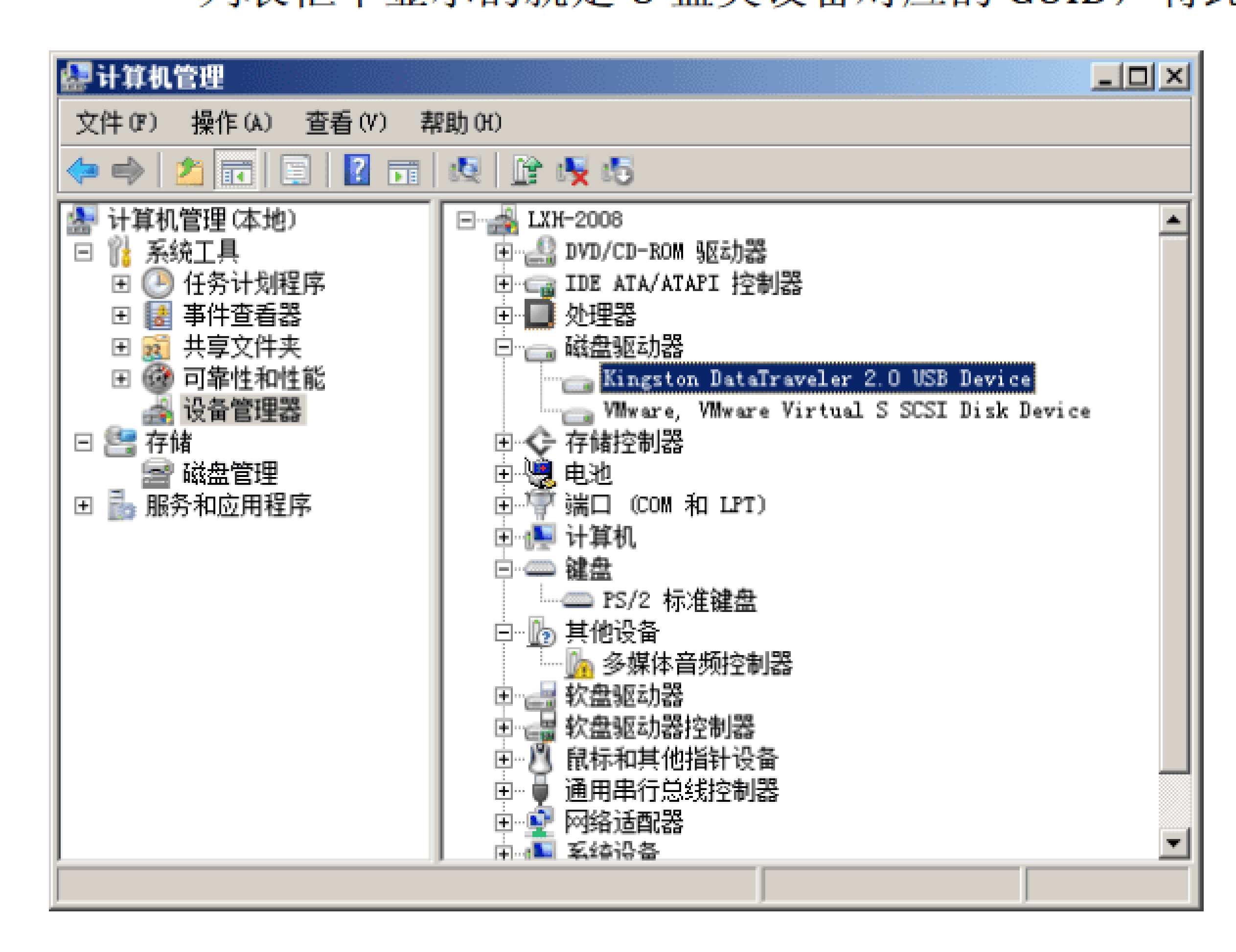


图 4-33　“计算机管理”窗口

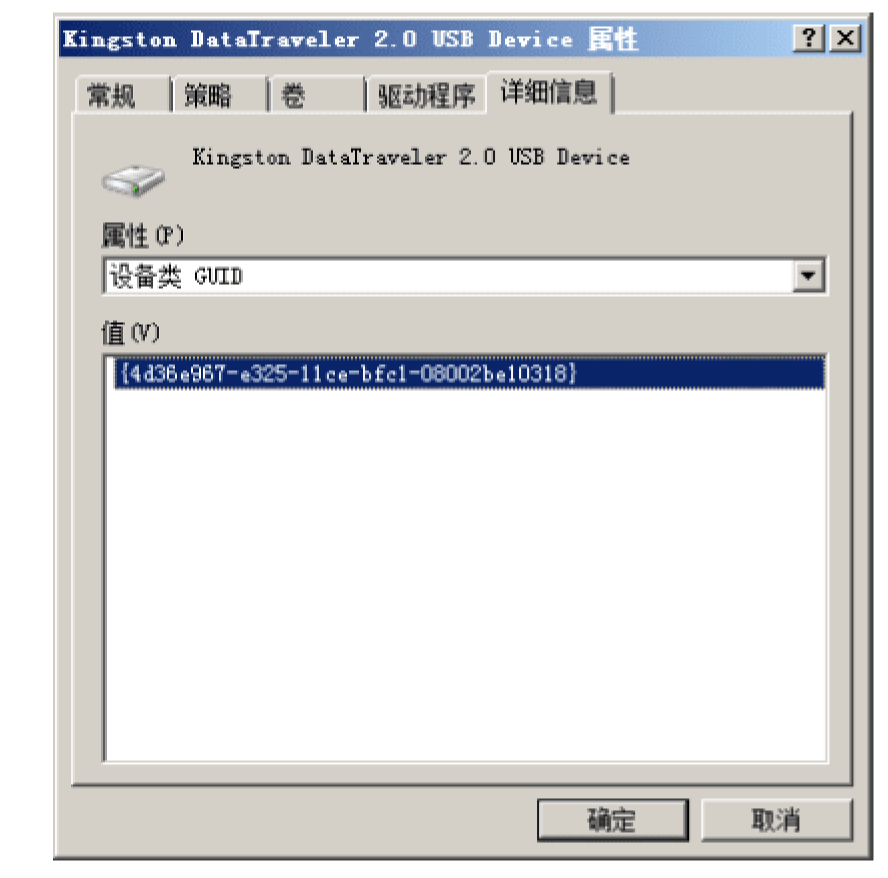


图 4-34　“详细信息”选项卡

③ 单击“确定”按钮，关闭对话框。

④ 在组策略管理器窗口中，依次展开“计算机配置”→“管理模板”→“系统”→“设备安装”→“设备安装限制”，显示如图 4-35 所示的窗口。

⑤ 双击“阻止安装与下列任何设备 ID 相匹配的设备”策略，显示如图 4-36 所示的对话框，选择“已启用”单选按钮。

⑥ 单击“显示”按钮，显示“显示内容”对话框，默认此列表为空白。单击“添加”按钮，显示“添加项目”对话框，将复制到粘贴板的 U 盘类设备 GUID，粘贴到“输入要添加的项目”文本框中即可，如图 4-37 所示。

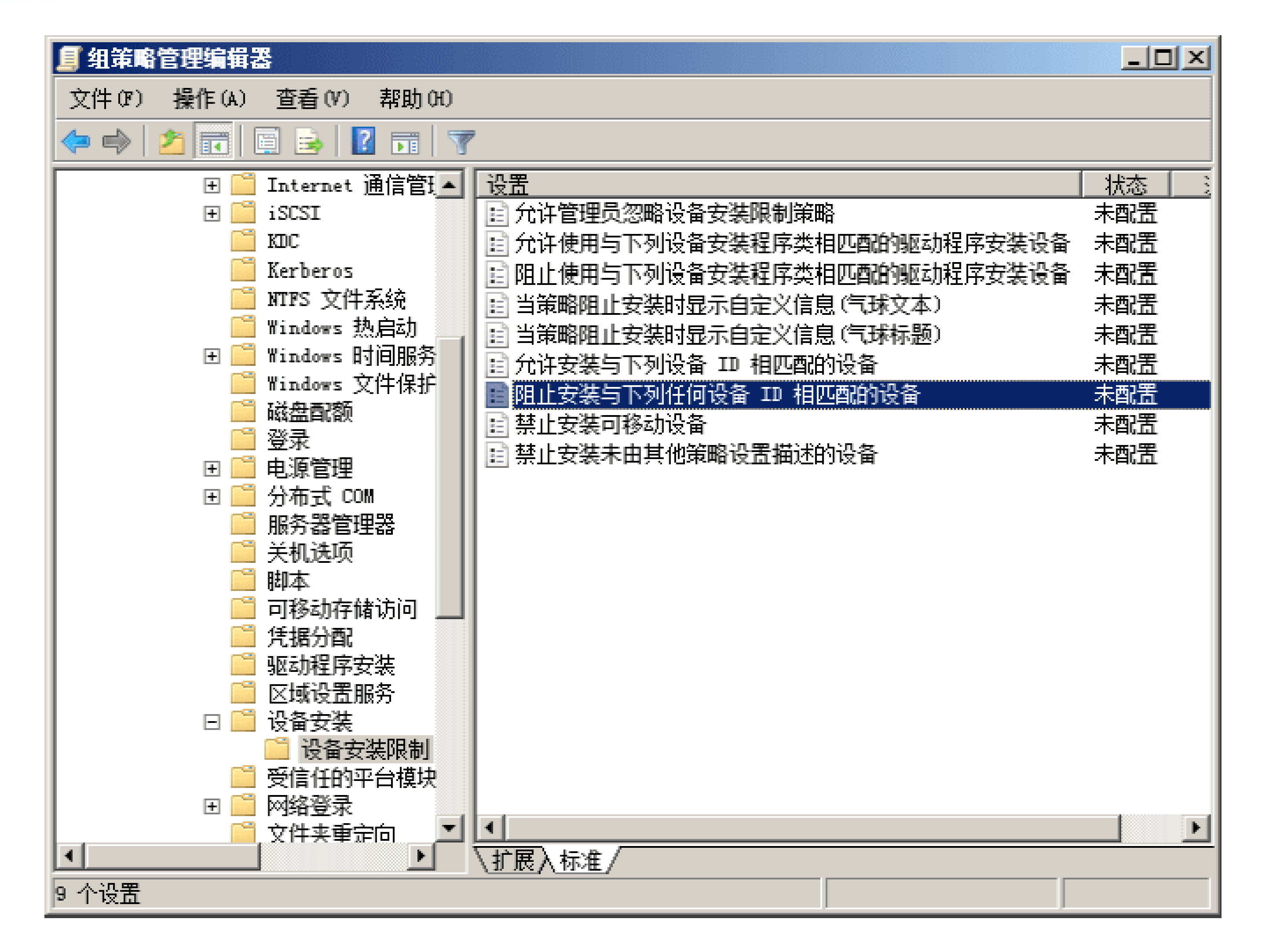


图 4-35 “组策略管理编辑器”窗口

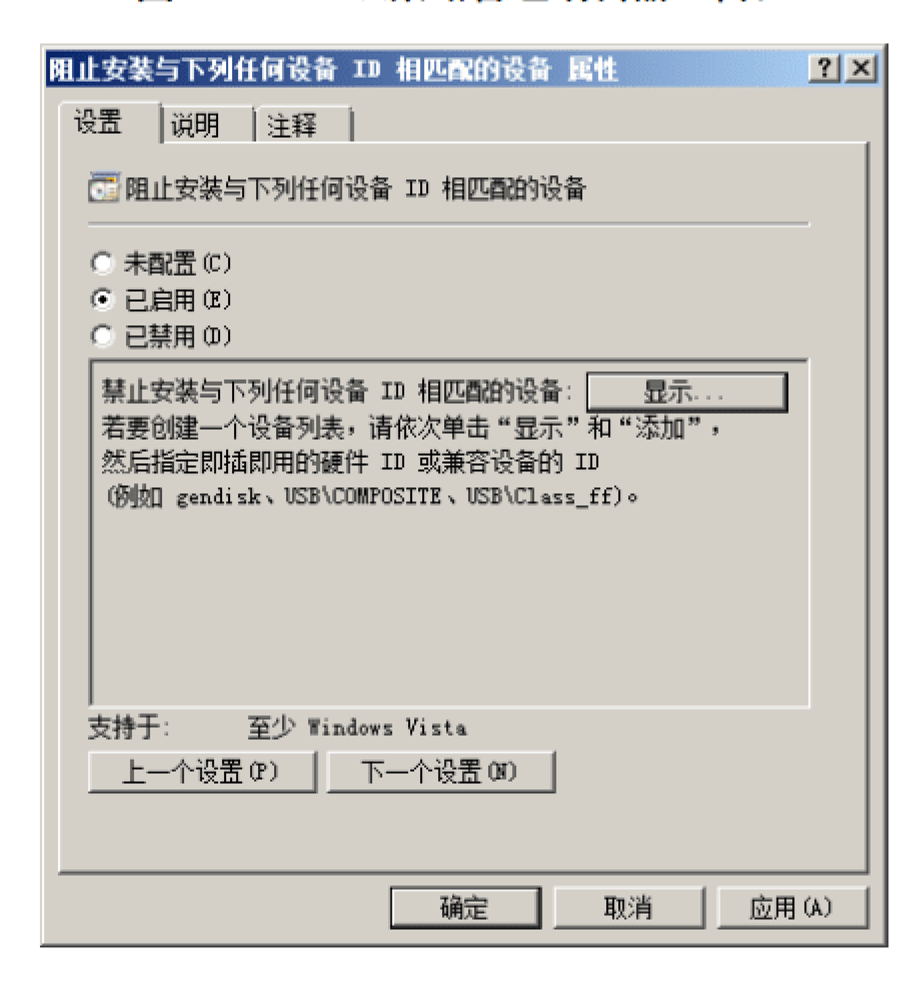


图 4-36 “阻止安装与下列任何设备 ID 相匹配的设备 属性”对话框

⑦ 连续单击“确定”按钮，保存设置即可。由于以上策略只是阻止使用 U 盘类设备，所以应用此策略后，用户仍可以将 U 盘插入 USB 接口，并且系统会自动为其安装驱动程序，但是在资源管理器中打开时，会发现 U 盘对应的可用磁盘空间为 0，不会显示任何数据，如图 4-38 所示。

这些措施，并不能从根本上解决核心数据的安全问题。恶意用户仍然可以通过电子邮件发送数据，并且，如果管理员的话，具备工作站或服务器的物理操作权限，则盗取数据更是易如反掌。所以说，最完美的解决方案是，确保核心数据的访问权限，而不是仅仅依靠组策略。



注意：如果在应用设备限制策略之前，用户已经将移动设备安装到系统中，则不能阻止用户的正常应用，该策略会在用户取下设备并再次安装移动设备时生效。




图 4-37　“添加项目”对话框

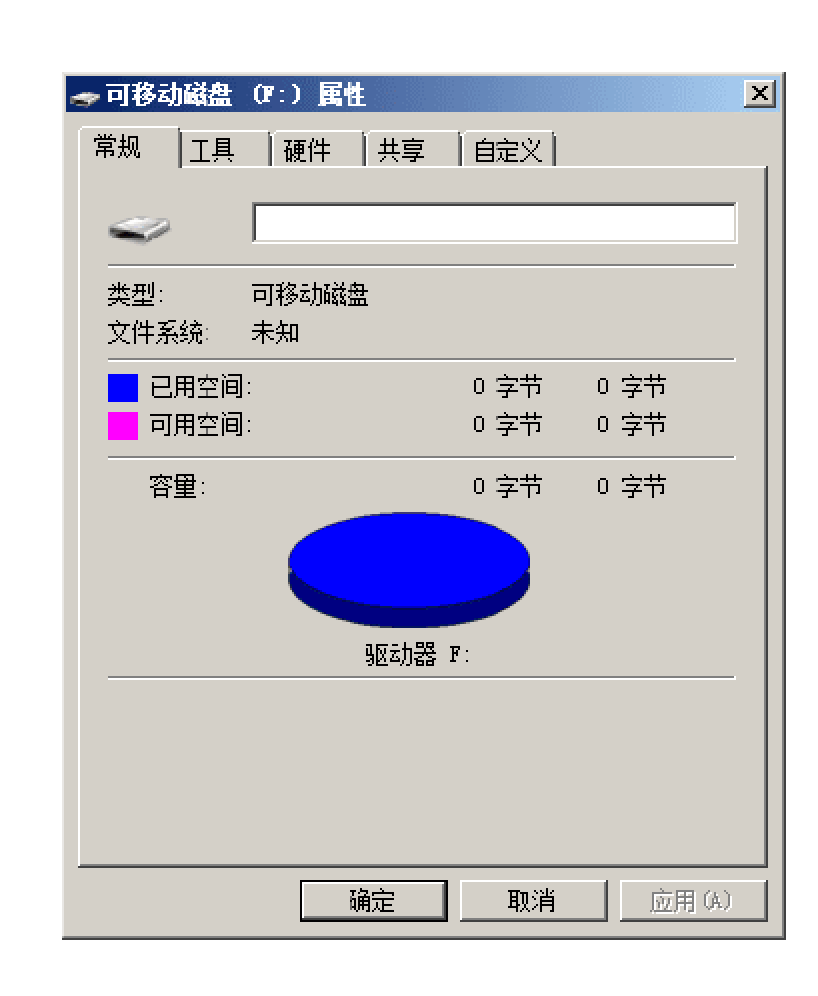


图 4-38　U 盘当前不可用

4.4　软件限制策略

软件限制策略主要用于控制应用程序的安装，如间谍软件、恶意程序等，可以为策略作用域下用户的软件使用进行限制。顾名思义，软件限制策略就是限制某些软件的使用。使用组策略的限制软件策略，可以通过规则标识并设置安全级别来指定软件是否运行，从而达到客户端计算机系统的可管理性、安全性。使用目的是控制不信任的和不被允许的软件在网络内的非法使用。

4.4.1　软件限制策略简介

使用软件限制策略，可通过标识并指定允许运行的软件来保护计算机环境免受不信任软件的侵袭。可以为组策略对象定义“不受限的”或“不允许的”的默认安全级别，从而决定是否在默认情况下允许软件运行。通过为特定软件创建软件限制策略规则，可以相对于默认安全级别做出例外安排。软件限制策略使用规则来标识和控制软件的运行方式。可以通过软件程序的哈希、证书、路径或其所驻留的 Internet 区域对其进行标识。对软件进行了标识后，可以决定是否允许运行。

软件限制策略可应用于计算机或用户，这取决于是修改了“计算机配置”中的设置还是“用户配置”中的设置。软件限制策略是通过组策略得以应用的。需要将策略设置应用于组策略对象，该对象与本地计算机、站点、域或组织单位相连。如果应用了多个策略设置，将遵循以下的优先级顺序(从低到高)：

- 本地计算机策略。
- 站点策略。
- 域策略。
- 组织单位策略。

所有策略设置在重新启动计算机后都会被刷新。修改策略设置时，在工作站或服务器上将每 90 分钟刷新一次，而在域控制器上将每 5 分钟刷新一次。不管是否更改了策略设置，它们都会每 16 小时刷新一次。通过先运行强制刷新组策略命令 gpupdate /force，然后注销计算机并重新登录来刷新策略设置。

软件限制策略中的规则标识一个或多个应用程序，以指定是否允许其运行。软件限制策略使用下列 4 个规则来标识软件：

- 哈希规则。使用可执行文件的加密密钥。
- 证书规则。用软件发布者为.exe 文件提供的数字签名证书。
- 路径规则。使用.exe 文件位置的本地路径、通用命名约定(UNC)路径或注册表路径。
- 区域规则。使用可执行文件源自的 Internet 区域。

使用软件限制策略可以实现以下目的：

- 控制软件在系统中的运行能力。
- 允许用户在多用户计算机上仅运行特定文件。
- 决定可以在计算机中添加信任的发布者的用户。
- 控制软件限制策略是作用于所有用户，还是仅作用于计算机上的某些用户。
- 阻止任何文件在本地计算机、组织单位、站点或域中运行。

4.4.2 安全级别设置

使用软件限制策略可以标识并指定允许运行的软件，以便保护计算机环境不会受到不可信代码的攻击。使用软件限制策略时，可以为组策略对象(GPO)定义系统默认的安全级别的一种，不受限的、不允许的或基本用户，使得在默认情况下或者允许软件运行，或者不允许软件运行，或者以用户账户身份而定。

1. 创建软件限制策略

默认情况下，Windows Server 2008 并没有配置软件限制策略，在“本地组策略编辑器”窗口中，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”选项，显示如图 4-39 所示的窗口。如果是在 Windows 域控制器上，编辑作用于站点或组织单位的组策略，则在“用户配置”→“策略”→“Windows 设置”→“安全设置”→“软件限制策略”分支中，同样可以创建软件限制策略(以 Windows Server 2008 域控制器为例)。

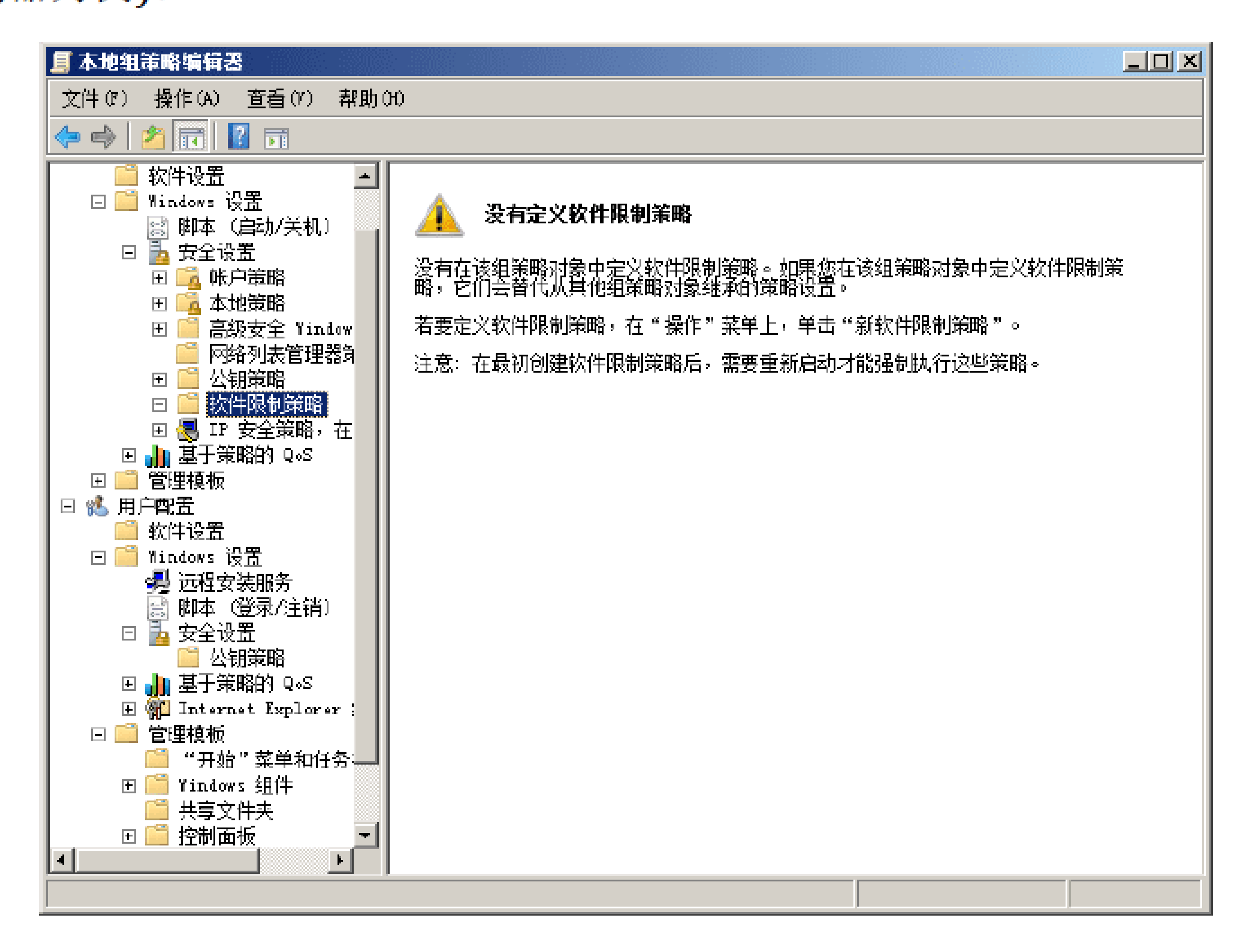


图 4-39 软件限制策略

右击“软件限制策略”并选择快捷菜单中的“创建软件限制策略”命令，系统将自动完成策略类型的构建，右侧窗口中即可显示可以配置的策略项目，如图 4-40 所示。

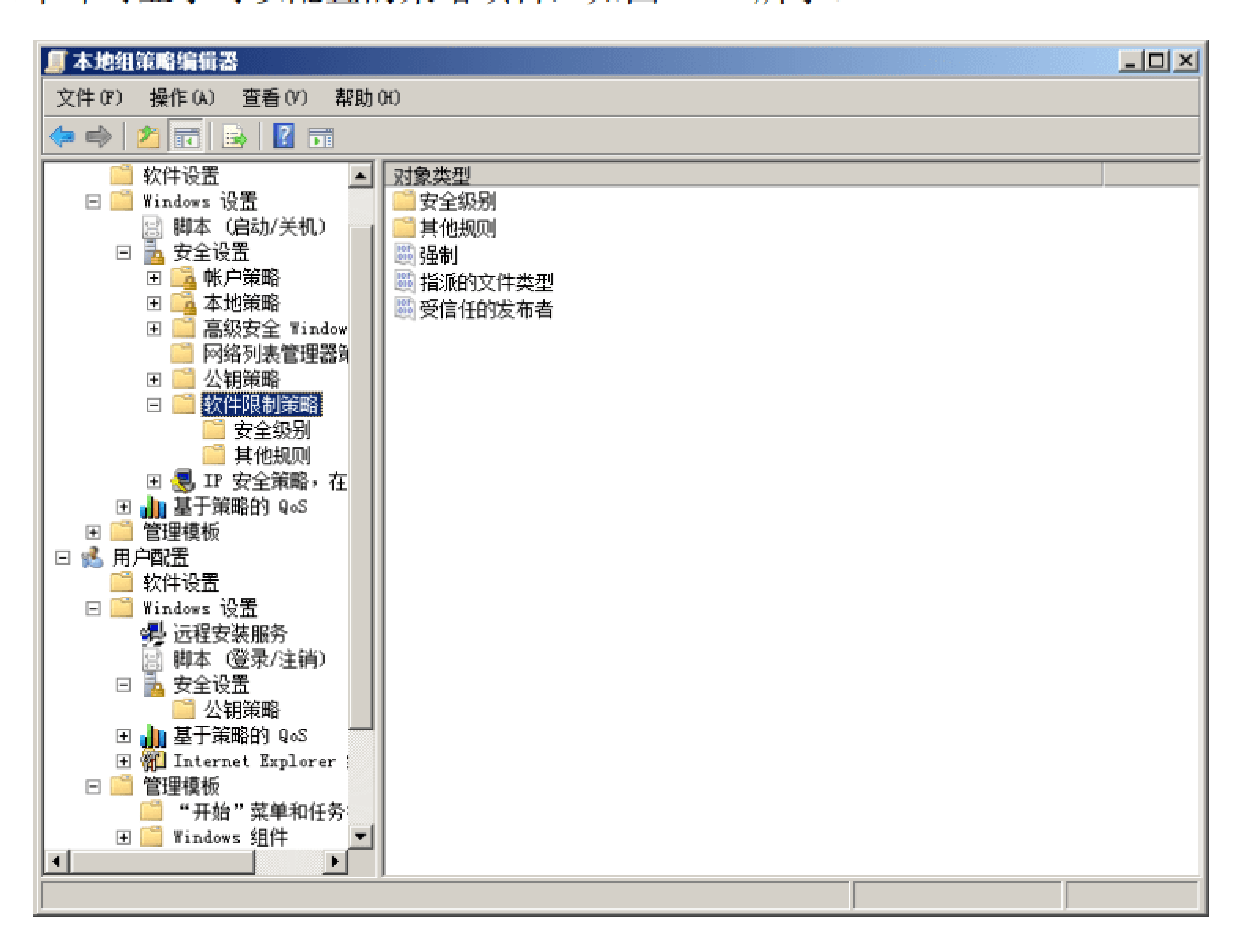


图 4-40　创建软件限制策略

2. 设置安全级别

安全级别指的是操作系统对应用策略所具备的访问级别，创建软件限制策略后，继续展开“安全级别”，显示如图 4-41 所示窗口。默认情况下，Windows Server 2008 系统中包括如下 3 种安全级别。

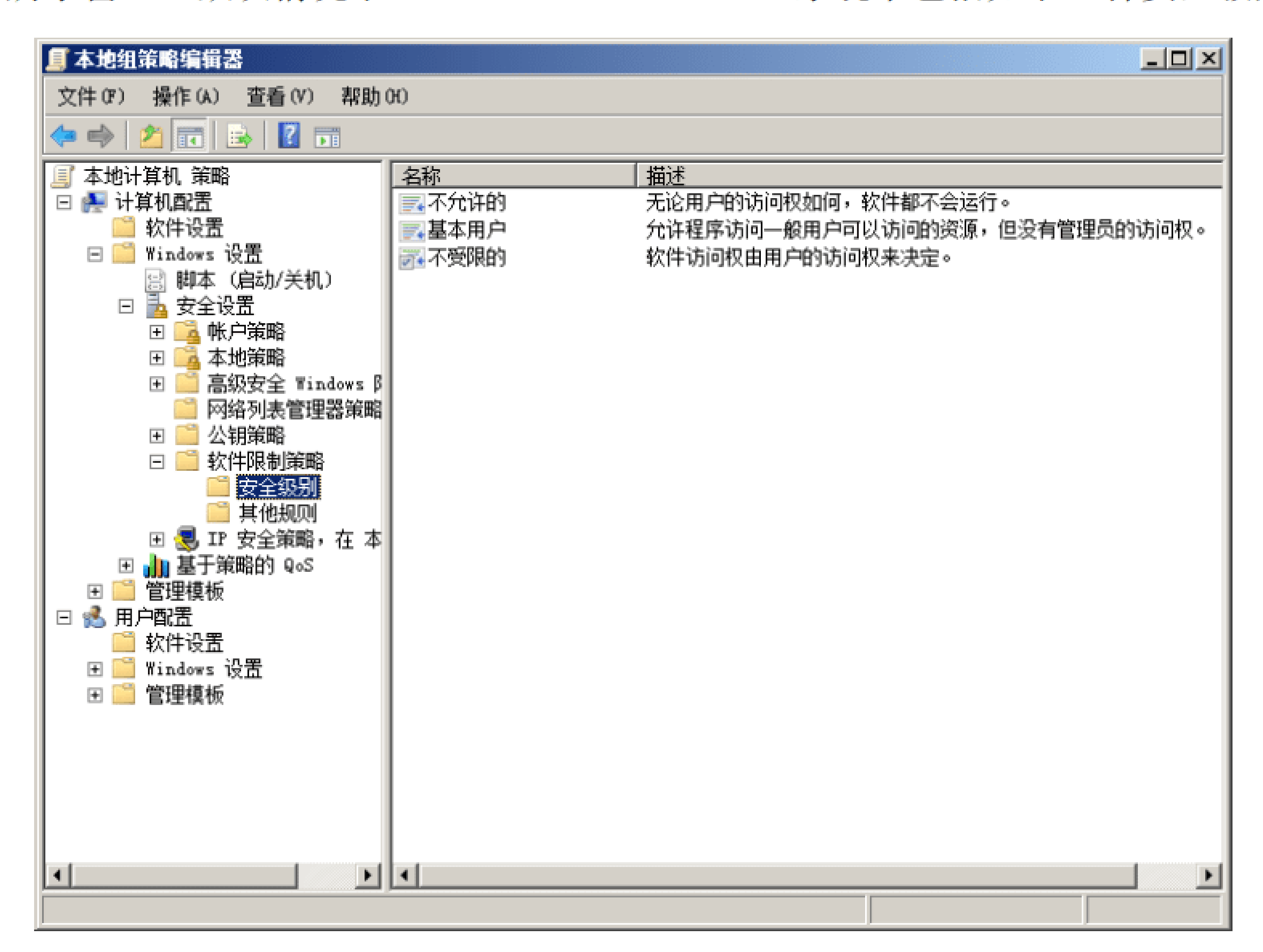


图 4-41　设置安全级别

- 不允许的。无论用户的访问权限如何，软件都不会运行。
- 基本用户。允许程序访问一般用户可以访问的资源，但没有管理员的访问权。
- 不受限的。软件访问权由用户的访问权来决定。

其中，“基本用户”是 Windows Server 2008 系统新增的安全级别。Windows Server 2008 的默认设置均为“不受限的”，即软件访问权限由用户账户自身的权限决定。

Windows 系统的默认安全级别为“不受限的”，管理员可根据需要修改其他默认安全级别。

① 双击“不允许的”项目，显示如图 4-42 所示的“不允许的 属性”对话框，当前状态为“不是默认级别”。

② 单击“设为默认”按钮，显示如图 4-43 所示的“软件限制策略”对话框，提示所选择的默认等级比当前默认等级还要严格，更改后可能会导致一些应用程序停止工作。

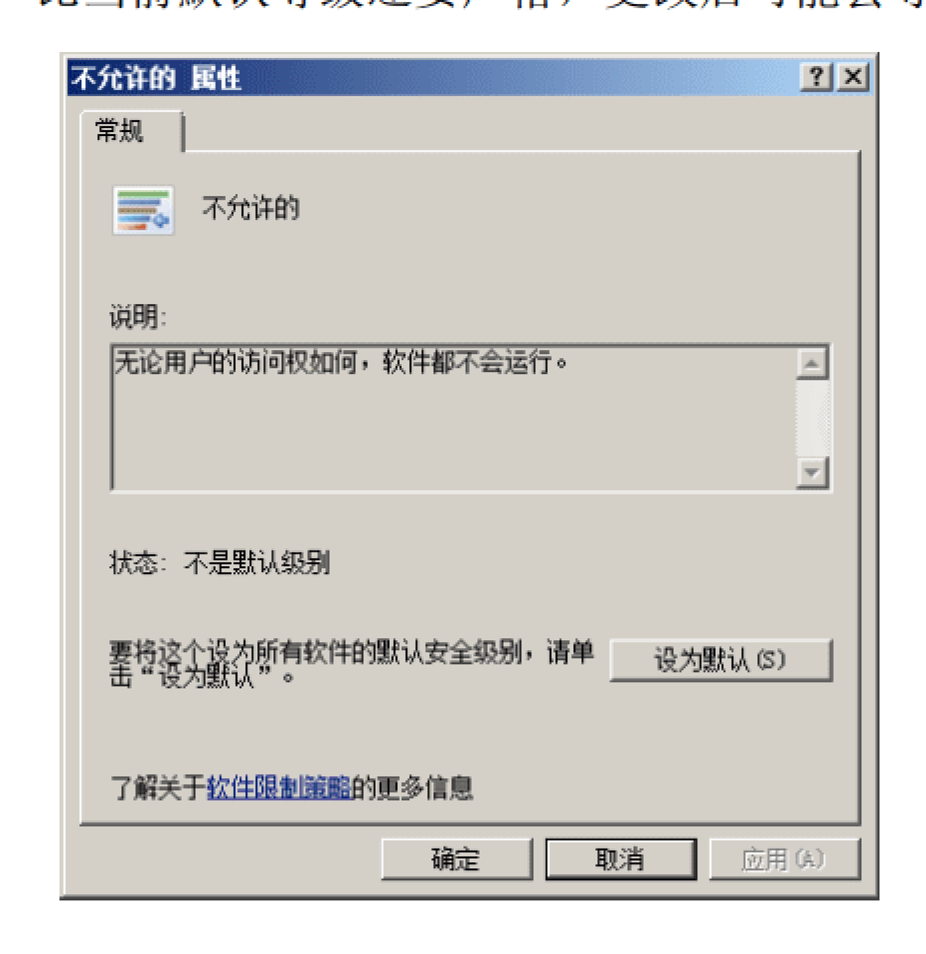


图 4-42 “不允许的 属性”对话框

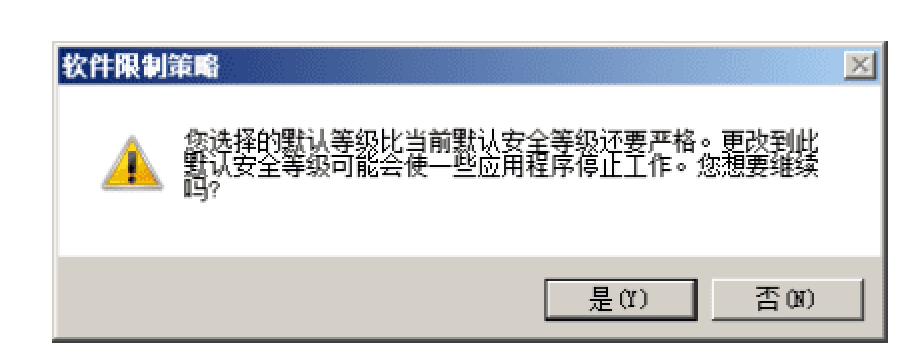


图 4-43 “软件限制策略”对话框

③ 单击“是”按钮，确认设置即可。返回“不允许的 属性”对话框，单击“确定”按钮，保存设置。

3. 设置路径规则

路径规则用于指定程序的文件夹路径或完全限定路径。当路径规则指定文件夹时，将匹配该文件夹中包含的任何程序以及相关子文件夹中包含的任何程序。路径规则既支持本地路径也支持 UNC 路径。

(1) 应用程序路径规则

路径规则允许对软件所在的路径进行标识，还允许使用软件的注册表路径规则。由于路径规则软件限制策略是按照软件所在的路径指定的，路径移动后，该软件限制策略将不再适用。

管理员必须在路径规则中定义用于启动特定应用程序的所有目录。例如，如果管理员在桌面上创建了一个用于启动应用程序的快捷方式，则在路径规则中，用户必须能够同时访问可执行文件路径和快捷方式路径才能运行该应用程序。试图仅使用这两个路径之一来运行应用程序将触发“Software Restricted”警告。

默认情况下，所有应用程序使用%ProgramFiles%变量作为安装目录，如果将该变量设置为不同驱动器上的其他目录，某些应用程序仍会将文件复制到原来的%Program Files%子目录中。因此，最好将路径规则定义到默认目录位置。

(2) 注册表路径规则

许多应用程序将其安装文件夹或应用程序目录的路径存储在系统注册表中。有些应用程序可以安装在文件系统中的任何位置，管理员可以创建路径规则来查找这些应用程序对应的注册表项。

使用特定文件夹路径或环境变量可能不会很容易地标识这些位置。但是，如果程序将其应用程序目录存储在注册表中，则可以创建一个路径规则，该路径规则将使用注册表中所存储的值，格式为：%<Registry Hive>\<Registry Key Name>\<Value Name>%。

如果将默认规则设置为“不允许的”，将设置 4 个注册表路径，以便操作系统能够访问系统文件以执行正常操作。创建这些注册表路径规则是为了避免将自己和所有其他用户锁定在系统之外。这些注册表规则被设置为“不受限的”。只有高级用户才可以修改或删除这些规则。注册表路径规则设置如下所示：

- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SystemRoot%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SystemRoot%*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%\System32*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

(3) 路径规则建议

使用表 4-3 可以确定最适合于应用程序的用户和环境的路径规则。

表 4-3　任务与推荐规则

任　务	推荐规则
允许或不允许特定程序版本	哈希规则 浏览到文件以创建哈希
标识始终安装在同一位置的程序	带有环境变量的路径规则 %ProgramFiles%\Internet Explorer\iexplore.exe
标识可以安装在客户端计算机上的任何位置的程序	注册表路径规则 %HKEY_LOCAL_MACHINE\SOFTWARE\ ComputerAssociates\InoculateIT\6.0\Path\HOME%
标识中央服务器上的一组脚本	路径规则 \\SERVER_NAME\Share
标识一组服务器上的一组脚本	带有通配符的路径规则
例如，DC01、DC02 和 DC03	\\DC??\Share
禁止所有.vbs 文件，但登录脚本目录中的.vbs 文件除外	带有通配符的路径规则 *.VBS 设置为“不允许的” \\LOGIN_SRV\Share*.VBS 设置为“不受限的”
不允许由病毒安装的名称始终为 flcss.exe 的文件	路径规则 flcss.exe 设置为“不允许的”
标识一组可以在任何位置运行的脚本	证书规则 使用证书对脚本进行数字签名
允许从受信任的 Internet 区域站点安装软件	区域规则 将“受信任的站点”设置为“不受限的”

(4) 注册表路径限制实施

① 单击“开始”按钮，在“开始搜索”文本框中，输入 regedit 并按 Enter 键，打开“注册表编辑器”窗口，找到想要设置路径规则的应用程序对应的注册表项，如 mmc。依次展开“HKEY_LOCAL_MACHINE”→“SOFTWARE”→“Microsoft”→“MMC”，右击 MMC 并选择快捷菜单中的“复制项名称”命令，如图 4-44 所示。

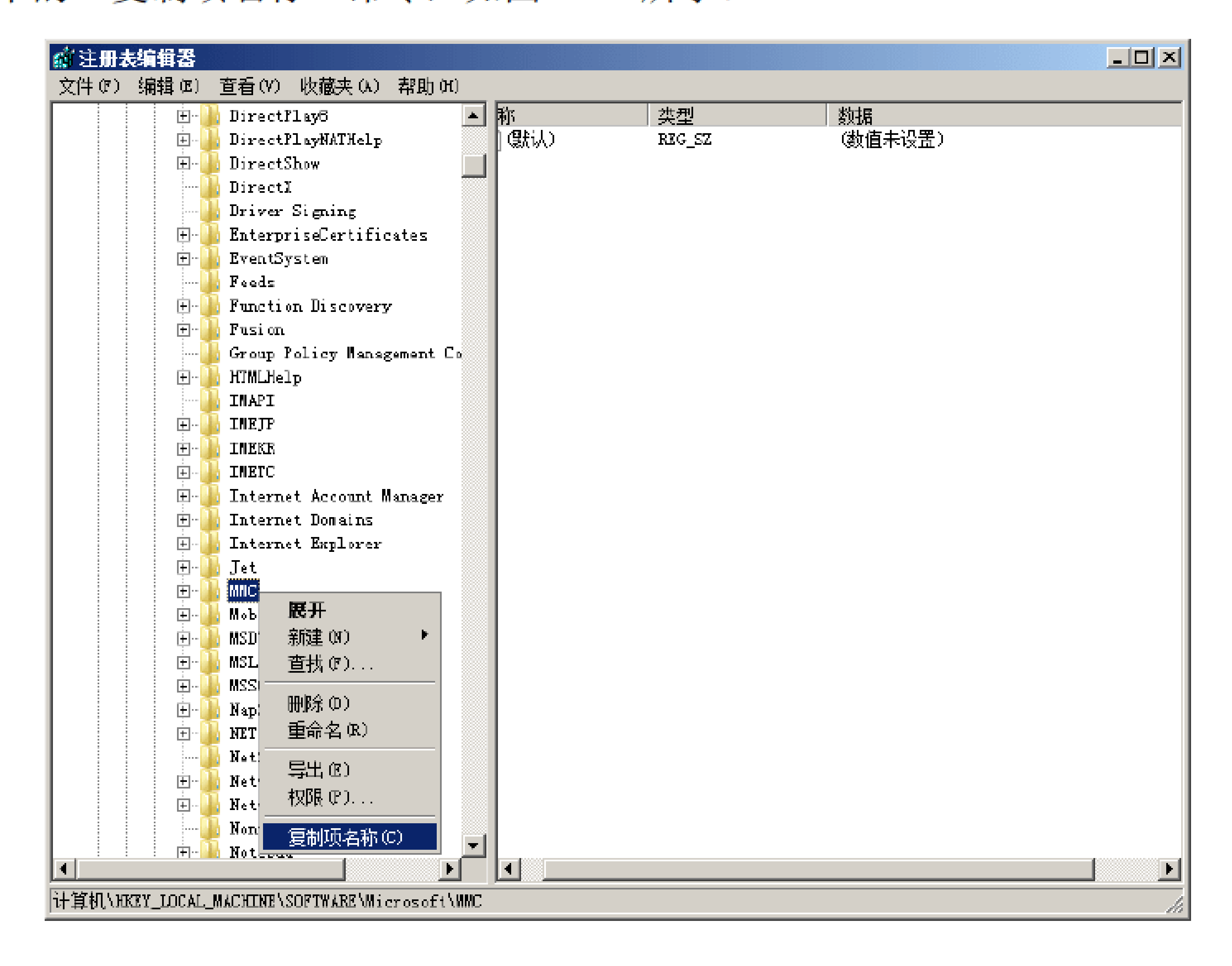


图 4-44 “注册表编辑器”窗口

② 在“本地组策略编辑器”窗口中，展开“软件限制策略”中的“其他规则”项目，如图 4-45 所示，系统默认已经设置了“%SystemRoot%”和“%ProgramFilesDir%”的路径限制，并且默认软件访问规则为“不受限的”。

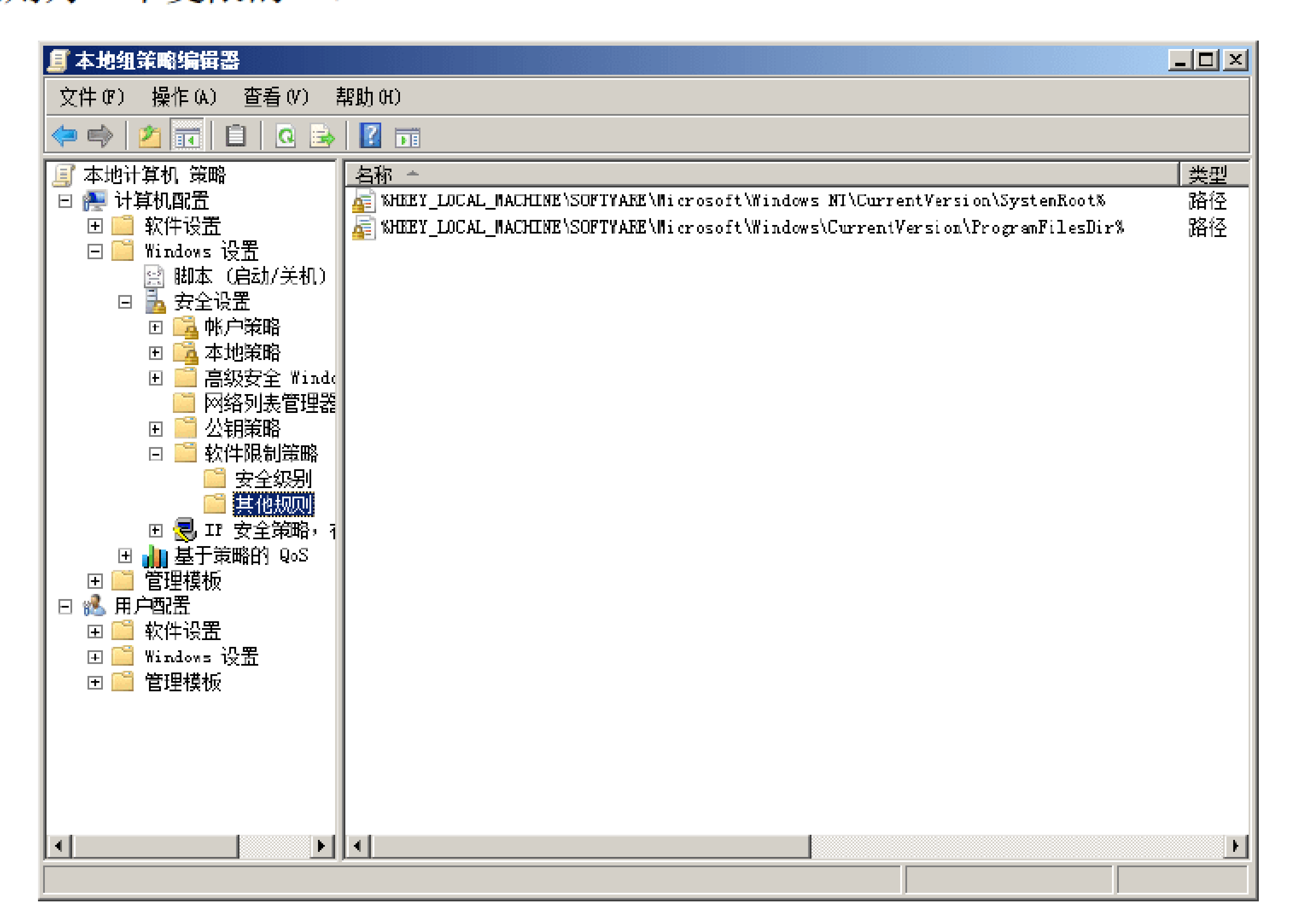


图 4-45 其他规则

③ 右击“其他规则”，选择快捷菜单中的“新建路径规则”命令，如图 4-46 所示。

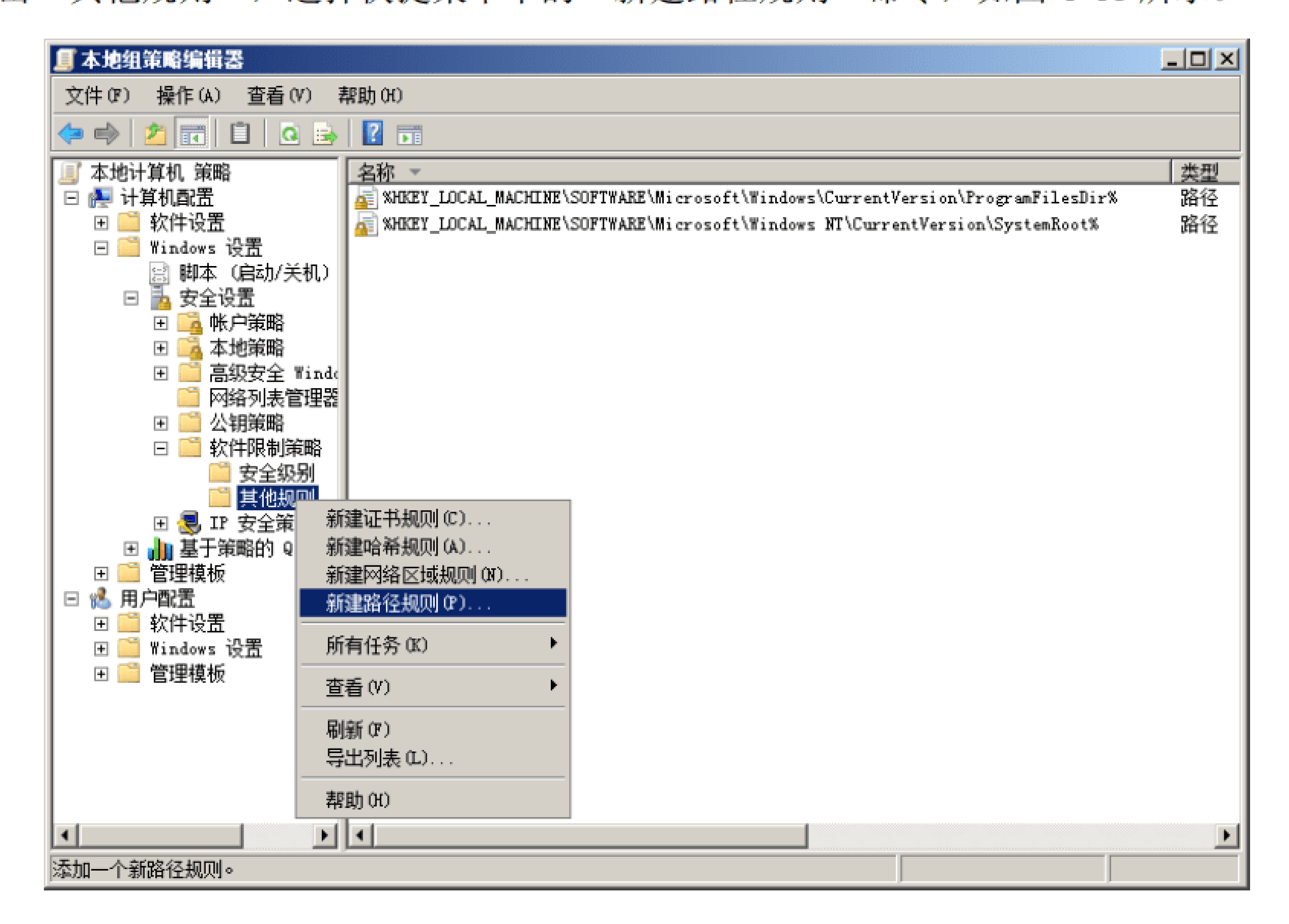


图 4-46 新建路径规则

④ 打开“新建路径规则”对话框，在“路径”文本框中，粘贴已复制的注册表项，并在首位加上“%”符号。在“安全级别”下拉列表中，选择想要设置的安全级别，如“不允许”，为了便于区分还可以在“描述”文本框中，输入相关描述信息，如图 4-47 所示。

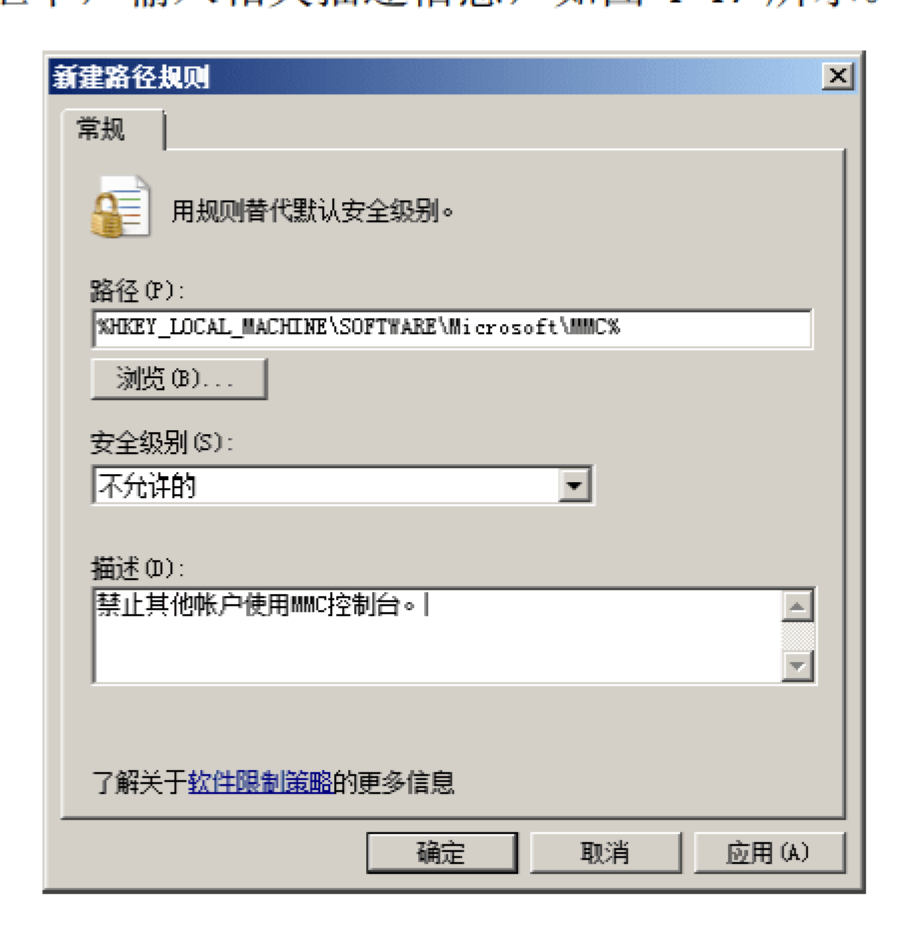
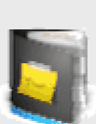


图 4-47 “新建路径规则”对话框



提示：除此之外，也可以单击“浏览”按钮，为本地计算机上的制定文件加设置访问规则。

⑤ 单击“确定”按钮，保存设置。

4.4.3 默认规则

创建软件限制策略的同时，Windows 系统已经默认安装了部分安全规则，包括强制、指派文件类型和受信任的发布者。

1. 强制

除非为组策略指定一个明显的强制规则，否则策略将对组下的所有用户生效。组策略允许对默认的安全级别做其他安排。如果默认的安全级别是“不允许的”，则可以为他指定一个新的规则，来允许软件的运行。对同一个软件可以使用多个规则，将由具备最高优先权的规则来指定软件是否运行。在“软件限制策略”右侧窗口中，双击“强制”显示如图 4-48 所示的“强制 属性”对话框。

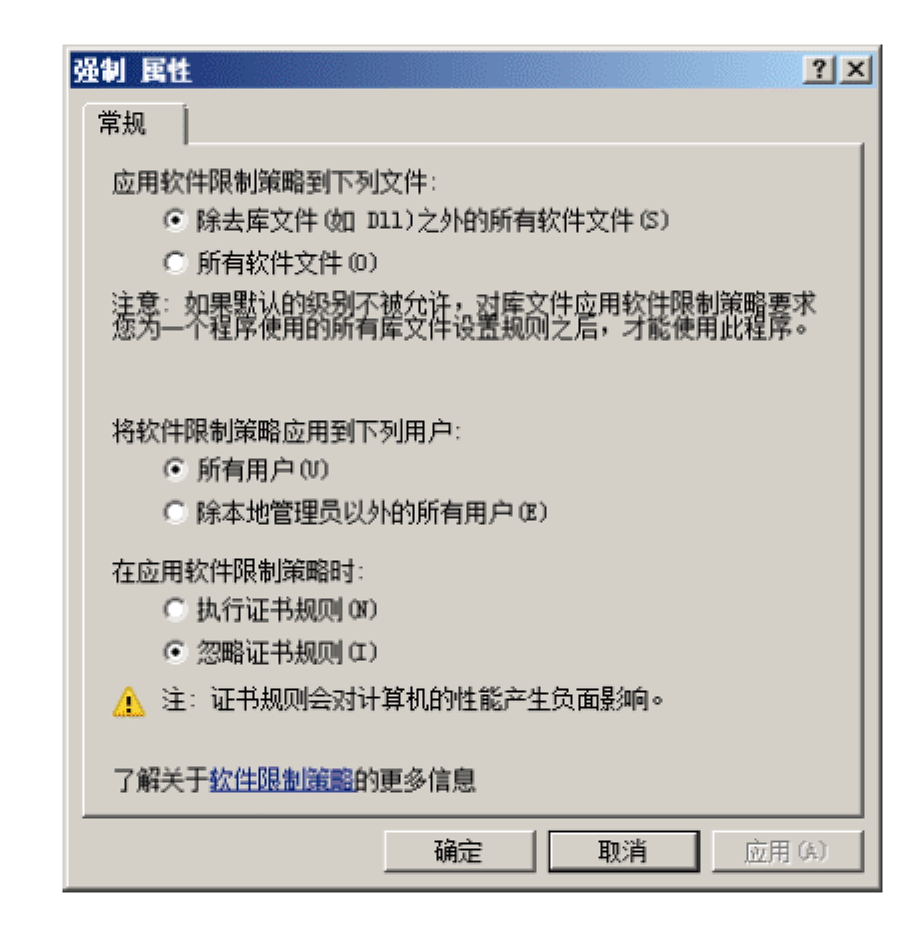


图 4-48 “强制 属性”对话框

(1) 应用软件限制策略到下列文件

在该选项区域，管理员可以对目标文件的类型进行限制，系统默认选择“除去库文件(如 DLL)之外的所有软件文件”单选按钮。一个应用软件，可能涉及很多后台的 DLL 文件，如果选择对所有软件文件进行限制，其他软件调用的时候可能会产生程序关联错误，建议使用除去库文件之外的所有软件文件，即保持系统默认设置。

大多数程序都由可执行文件和许多支持 DLL 文件组成。默认情况下，不会对 DLL 强制实施软件限制策略规则。这是针对大多数客户的推荐选项，下面列出了这样做的 3 个原因：

- 不允许主要可执行文件可以阻止程序运行，因此无需再阻止构成程序的 DLL。
- 由于 DLL 必须检查链接到应用程序的所有库，因此会降低系统性能。例如，如果用户在登录会话中运行了 10 个程序，则软件限制策略将评估每个程序。打开 DLL 检查后，软件限制策略将评估每个程序中的每个 DLL 负载。如果每个程序使用 20 个 DLL，这将导致 10 个可执行程序检查以及 200 个 DLL 检查，因此软件限制策略必须执行 210 次评估。Internet Explorer 之类的程序由可执行文件、iexplore.exe 和多个支持 DLL 组成。
- 将默认安全级别设置为“不允许的”，将强制系统不仅要标识主要可执行文件(在允许该程序运行之前)，还要标识作为.exe 文件组成部分的所有 DLL，这将加重系统负担。

(2) 将软件限制策略应用到下列用户

在该选项区域，管理员可以设置软件限制策略应用到的用户账户，默认为所有账户，但由于软件策略的应用可能会影响到管理员正常的系统管理和维护操作，因此，建议选择“除本地管理员以外的所有用户”单选按钮。

如果在链接到 Active Directory 中的对象的 GPO 中创建了软件限制策略，则建议拒绝将此 GPO 上的“应用组策略”权限授予 Administrators 组。

(3) 在应用软件限制策略时

在该选项区域，管理员可以设置应用软件限制策略时，是否执行证书规则，系统默认是不执行的。如

果本地计算机或所在网络中配置了证书服务器，则可以选择“执行证书规则”单选按钮，即执行软件限制策略的同时执行证书规则中的权限限制。需要注意的是，此时可能会占用过多的系统资源。

2. 指派文件类型

在“软件限制策略”右侧的对象类型列表中，双击“指派的文件类型”策略，显示如图 4-49 所示的“指派的文件类型 属性”对话框。该对话框列出了软件限制策略控制的文件类型，指派的文件类型将被视为可执行文件。例如，屏幕保护文件(.scr)便被视为可执行文件，因为在 Windows 资源管理器中双击该文件时，将作为程序被加载。

软件限制策略规则只适用于“指派的文件类型 属性”对话框列出的文件类型。如果环境使用要应用规则的文件类型，将该文件类型添加到列表中。例如，在“文件扩展名”文本框中输入“docx”，并单击“添加”按钮，即可将其添加至“指定的文件类型”列表中。

3. 受信任的发布者

在“软件限制策略”右侧的对象类型列表中，双击“受信任的发布者”显示如图 4-50 所示的“受信任的发布者 属性”对话框。选中“定义这些策略设置”复选框，管理员可以在这里配置哪些用户可以选择受信任的出版商，还可以确定在信任发布者之前执行哪些证书吊销检查(如果存在证书颁发机构)。系统默认设置为“允许所有管理员和用户管理用户自己的受信任的发布者”，及普通用户账户也可以管理自己受信任的发布者。在 Windows 域环境中，管理员还可以选择“允许企业管理员管理受信任的发布者”单选按钮，从而避免普通擅自更改自己受信任的发布者信息。



图 4-49　“指派的文件类型 属性”对话框

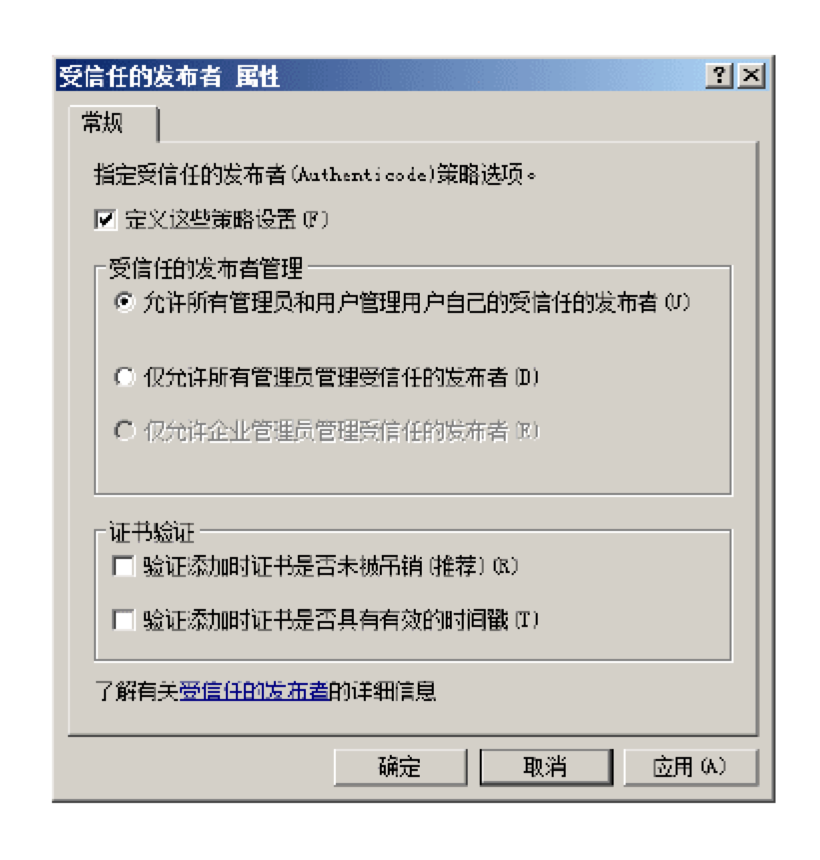


图 4-50　“受信任的发布者 属性”对话框

在“证书验证”选项区域，管理员可以根据需要并结合自己的实际情况，选择相应的验证方式。启用证书规则后，软件限制策略将检查证书吊销列表(CRL)，以确保软件的证书和签名有效，这样可能会造成签名程序启动时系统性能的下降。通过验证功能，可以配置与 ActiveX 控件以及其他签名内容相关的设置。

如表 4-4 所示显示了与 ActiveX 控件以及其他签名内容相关的受信任发布者选项。

表 4-4　受信任发布者选项

设置名称	任　务
企业管理员	用于只允许企业管理员进行有关签名活动内容的决策

续表

设置名称	任　务
本地计算机管理员	用于允许本地计算机管理员进行有关签名活动内容的所有决策
最终用户	用于允许用户进行有关签名活动内容的决策
发布者	用于确保软件发布者使用的证书未被吊销
时间戳	用于确保组织用于对活动内容加时间戳的证书未被吊销

4.5　IE 安全策略

Internet Explorer 内置的许多功能都允许管理员或者电脑使用者进行定制。在企业网络应用环境中，为了减少非法控件的下载、安全区域的定制、统一部署浏览器工具栏的定义等可以在基于活动目录的组策略应用中，集中部署 Internet Explorer 的应用。

4.5.1　阻止恶意程序入侵

在 Windows Server 2008 系统环境中使用 IE 浏览器上网浏览网页内容时，时常会有一些恶意程序不请自来，自动下载保存到本地计算机硬盘中，这样不但会白白浪费宝贵的硬盘空间资源，而且也会给本地计算机系统的安全带来威胁。在 Windows Server 2008 系统环境中，通过配置相关策略，即可禁止恶意程序自动下载保存到本地计算机硬盘中。

① 以管理员账户登录系统，打开“本地组策略编辑器”窗口。展开“计算机配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“安全功能”→“限制文件下载”，显示如图 4-51 所示窗口。

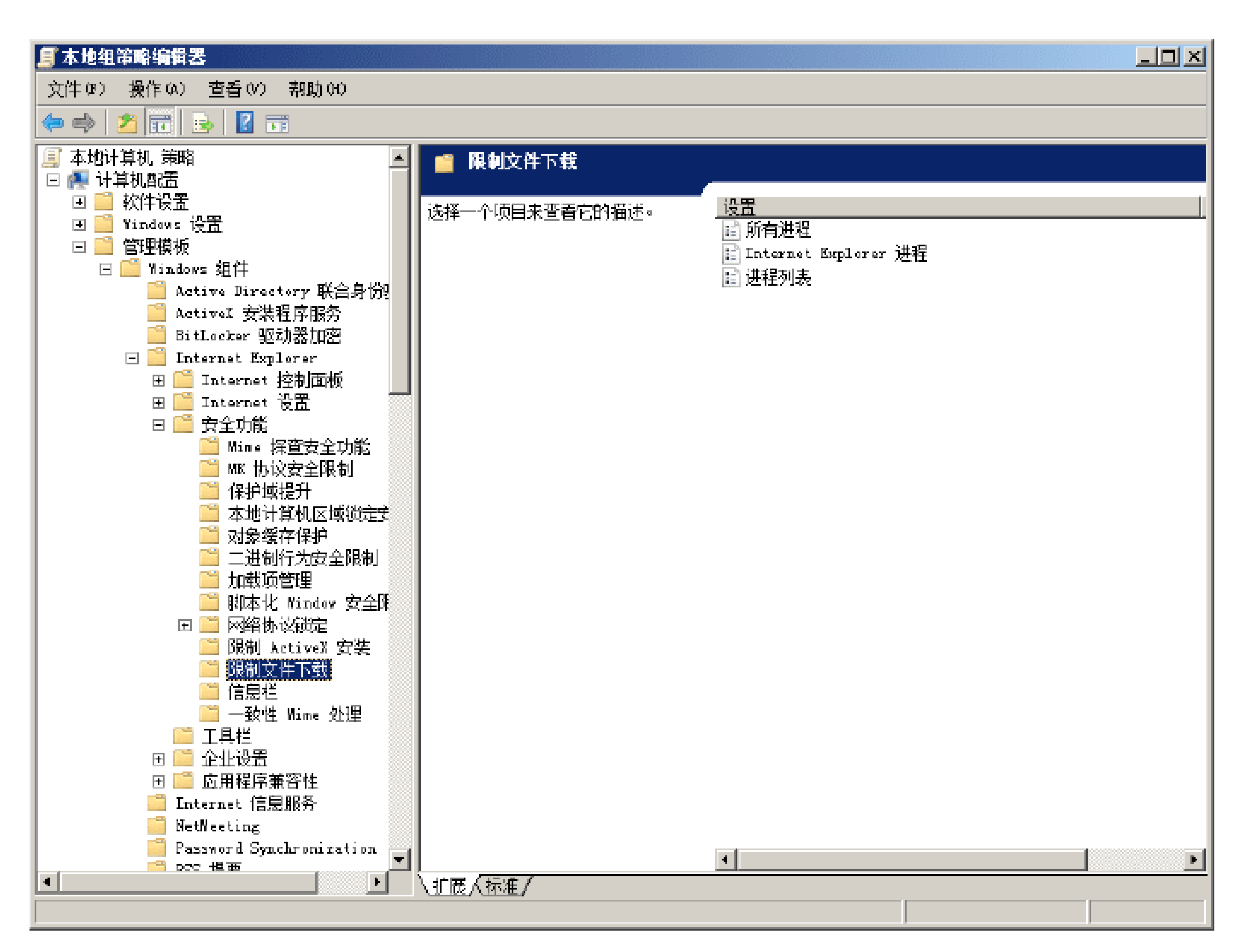


图 4-51　“本地组策略编辑器”窗口

② 双击“限制文件下载”子项中的“Internet Explorer 进程”组策略选项，显示如图 4-52 所示的

“Internet Explorer 进程 属性”对话框，选择“已启用”单选按钮。

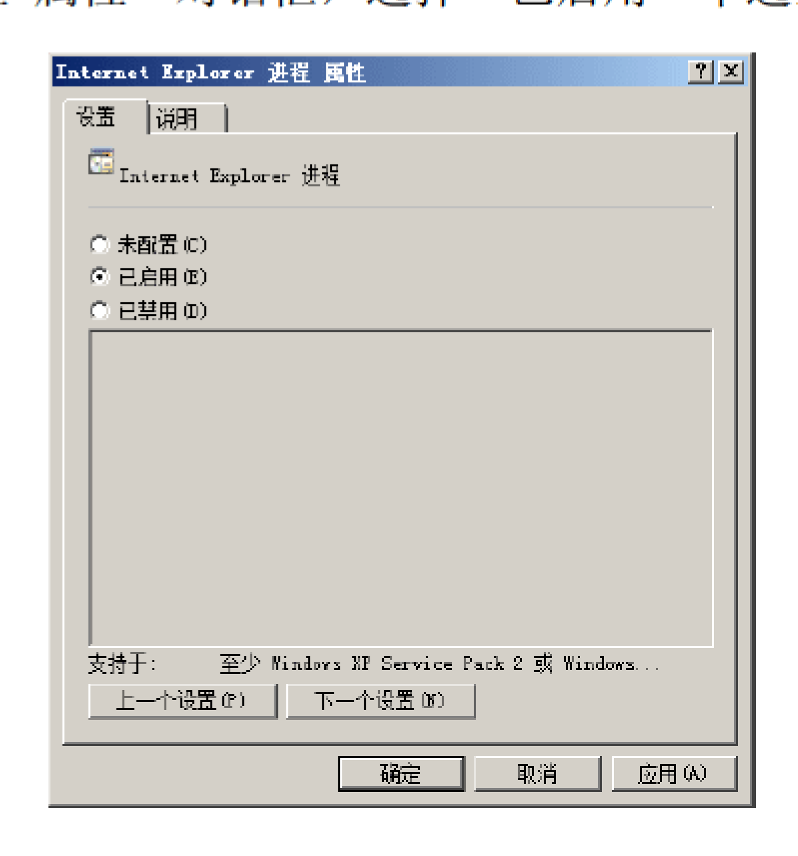


图 4-52　“Internet Explorer 进程 属性”对话框

③　单击“确定”按钮，保存设置。这样，Windows Server 2008 系统就会自动弹出阻止 Internet Explorer 进程的非用户初始化的文件下载提示，恶意程序也就无法通过 IE 浏览器窗口入侵本地计算机。

4.5.2　禁止改变本地安全访问级别

在一些公共场合的计算机上，不同的用户往往会根据需要随时更改 IE 浏览器的安全级别，但是如果安全级别过低，很可能导致潜藏在网络中的各种病毒或木马对本地计算机进行恶意攻击，从而可能造成本地系统运行缓慢或者无法正常运行的故障现象。为了用户随意更改本地计算机的安全访问级别，Windows Server 2008 系统允许用户通过相关设置，来保护本地系统的安全。

①　以管理员账户登录系统，打开“本地组策略编辑器”窗口。展开“计算机配置”→“管理模板”→“Windows 组件”→“Internet Explorer”→“安全功能”，显示如图 4-53 所示的窗口。

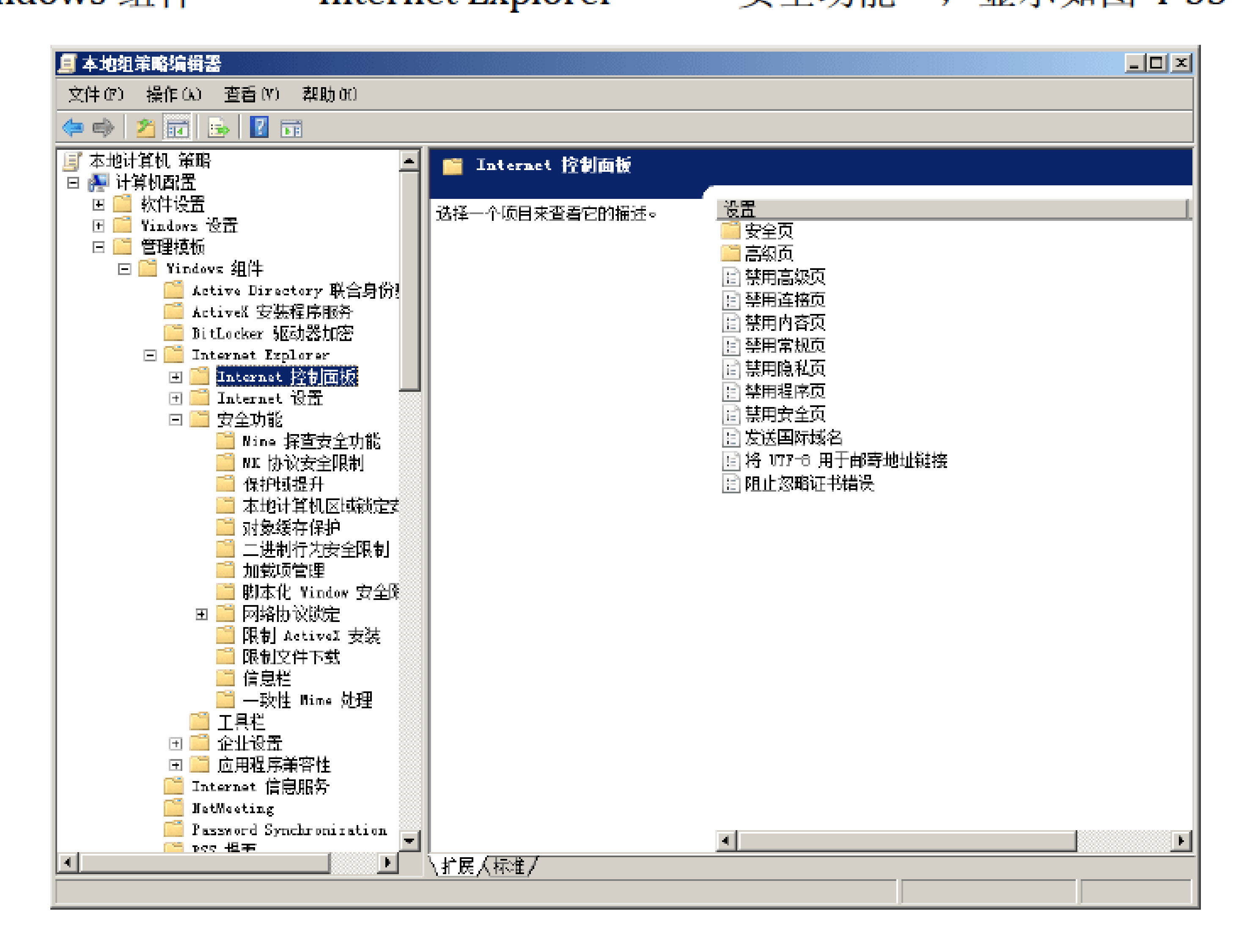


图 4-53　打开的“Internet 控制面板”窗口

② 双击右侧窗口中的“禁用安全页”，显示如图 4-54 所示的“禁用安全页 属性”对话框，选择“已启用”单选按钮。

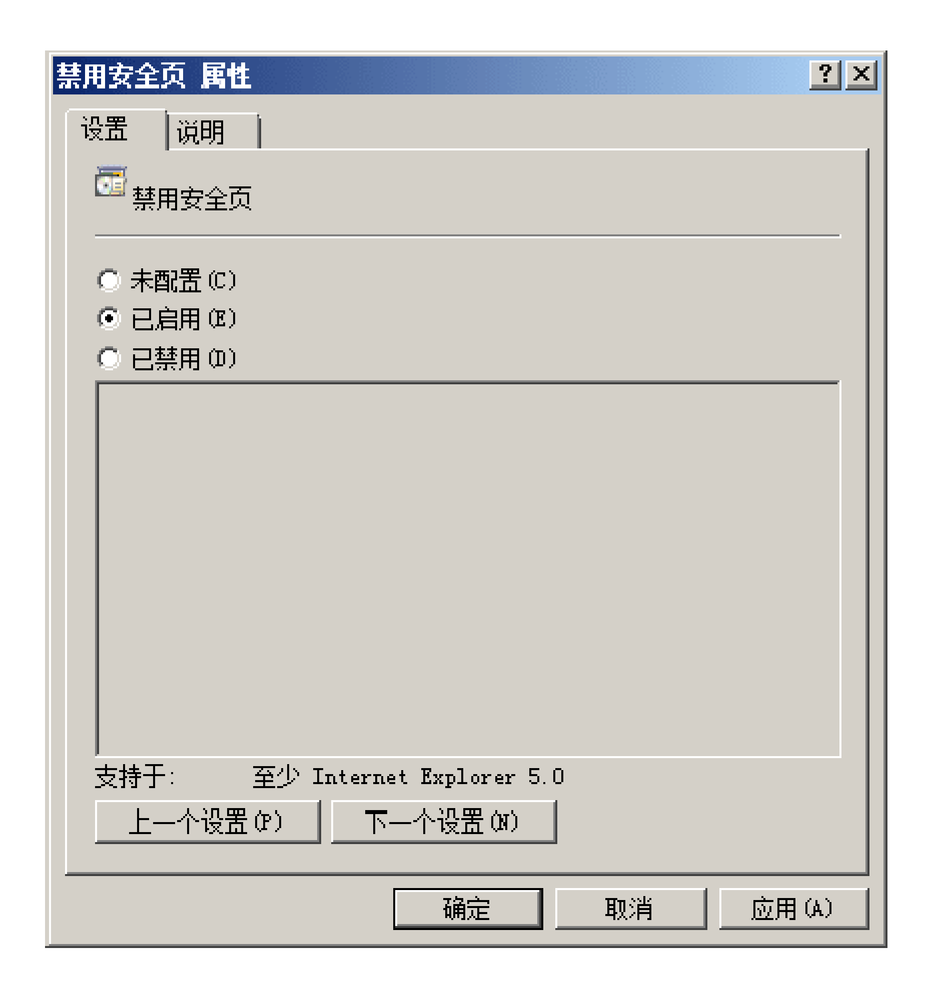


图 4-54 “禁用安全页 属性”对话框

③ 单击“确定”按钮，保存设置。此时，Internet Explorer 的安全设置页面就会被自动隐藏起来，其他用户就无法进入该安全标签设置页面，无法随意更改本地系统的安全访问级别，本地计算机系统的安全性即可得到有效保证。

第 5 章　用户账户安全

在 Windows Server 2008 系统中，包括多种用户账户，前面介绍过的 Administrator 只是其中比较关键的用户账户之一，除此之外，还包括标准账户、来宾账户等，在 Active Directory 中还包括普通成员账户、域管理员账户、企业管理员账户等。用户账户是通向系统和网络的大门，密码是开启网络大门的钥匙。用户账户的安全与否，将直接影响系统乃至整个网络的安全。

关键词

- 用户账户的管理
- 用户组的管理
- 用户权限的安全
- 用户环境安全
- 域用户配置文件安全

5.1 用户账户的管理

除管理员账户之外，还应为其他用户创建一些普通账户，如来宾账户、个人用户账户等。为了确保系统或网络的安全，普通用户账户的安全设置也是不可小视的，如果操作不当很容易导致安全漏洞。例如，管理员必须根据用户的实际身份和管理职能，及时调整其对应账户的身份。如果用户暂时离开网络，则可以先停用其账户，以免被滥用。

5.1.1 新建用户账户

在本地计算机或者 Windows 网络中，用户账户和用户是一一对应的。当需要将某项任务指派给用户时，首先应为其创建用户账户，并赋予适当的操作权限。在域环境中，当有新用户进入网络时，也需要在域控制器上为其创建对应的用户账户。账户安全工作应该从创建用户账户的操作开始。

1. 创建本地用户账户

① 以管理员账户登录系统，依次选择“开始”→“管理工具”→“计算机管理”命令，打开“计算机管理”窗口，依次展开“系统工具”→“本地用户和组”→“用户”选项，显示如图 5-1 所示的窗口。

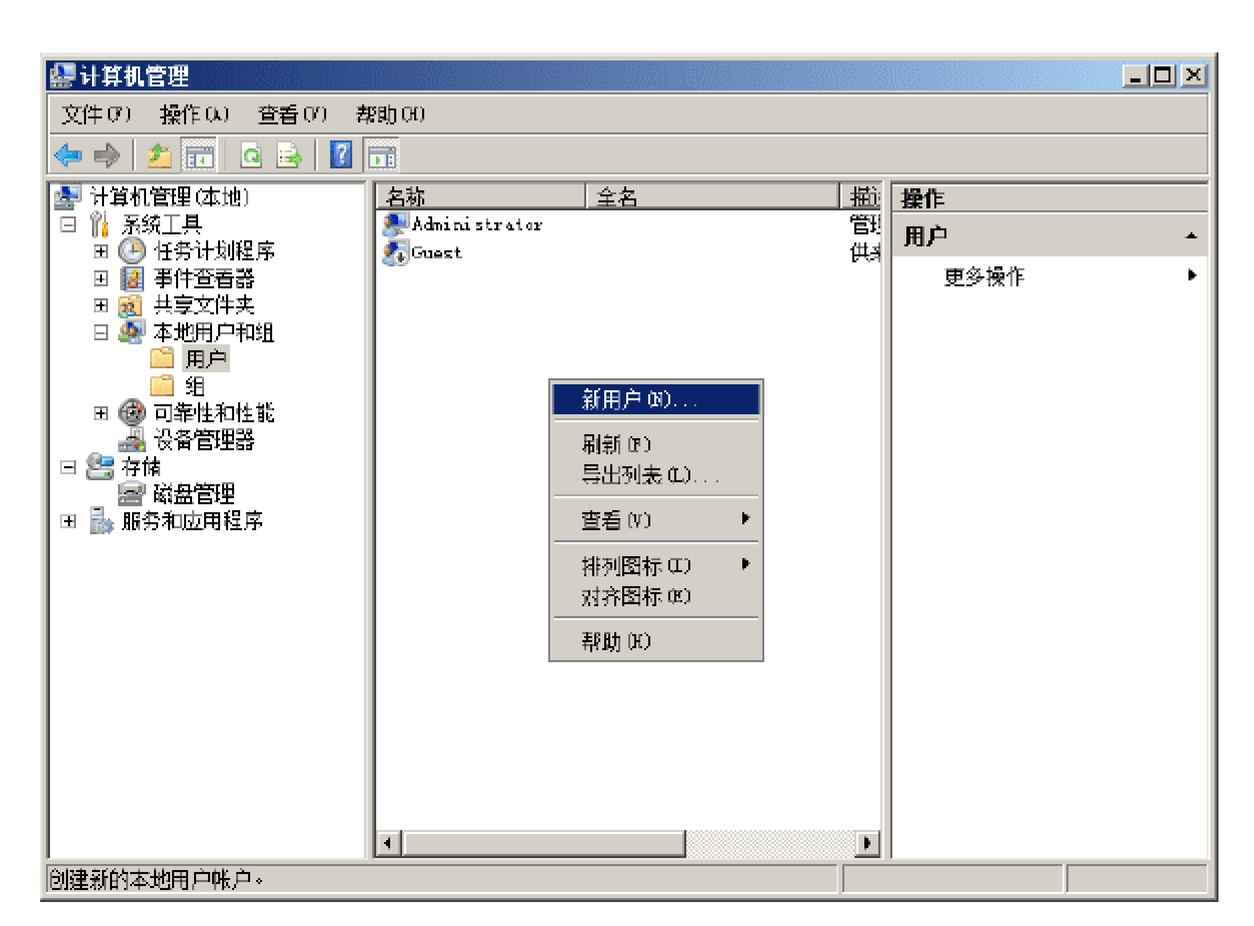


图 5-1 “计算机管理”窗口

② 在窗口空白处右击，选择快捷菜单中的“新用户”命令，打开如图 5-2 所示的“新用户”对话框。在“用户名”文本框中输入新用户名，在“密码”和“确认密码”文本框中，为该用户账户设置安全密码。除此之外，还包括如下几种可选操作：

- 用户下次登录时须更改密码。强制用户下次登录网络时更改密码，希望该用户成为唯一知道其密码的用户时，可以选中该复选框。
- 用户不能更改密码。阻止用户更改其密码。当希望保留对用户账户(如，来宾账户)的控制权时，或者该账户是由多个用户使用时，应当使用该选项。同时，必须取消选中“用户下次登录时须更改密码”复选框。

- 密码永不过期。防止用户密码过期，建议对“服务”账户启用该复选框，并且应使用强密码。
- 账户已禁用。如果选中该复选框，则禁用该用户账户。



提示： 如果某用户彻底脱离该计算机，则应当立即删除其账户，而不是简单的禁用。禁用账户只是暂停了该用户的使用，而该账户 ID 仍然存在。删除账户时，则连同其 ID 一同删除，即使再重新创建一个用户名完全相同的账户，其用户 ID 也已经不同了。

③ 单击“创建”按钮，即可创建一个新的用户账户。

2. 创建域用户账户

域环境中用户账户的创建，与本地账户略有不同，并且对账户安全的要求更加严格。默认情况下，域控制器已经启用了对用户账户密码安全的一些限制，包括禁止使用简单密码、空白密码、使用期限等。域管理员或者被委派相应权限的用户账户，才可以执行创建用户账户的操作。

① 在“服务器管理器”窗口中，展开指定域控制器下的“Active Directory 用户和计算机”选项，单击 Users，显示如图 5-3 所示的窗口，列出了系统默认用户账户。

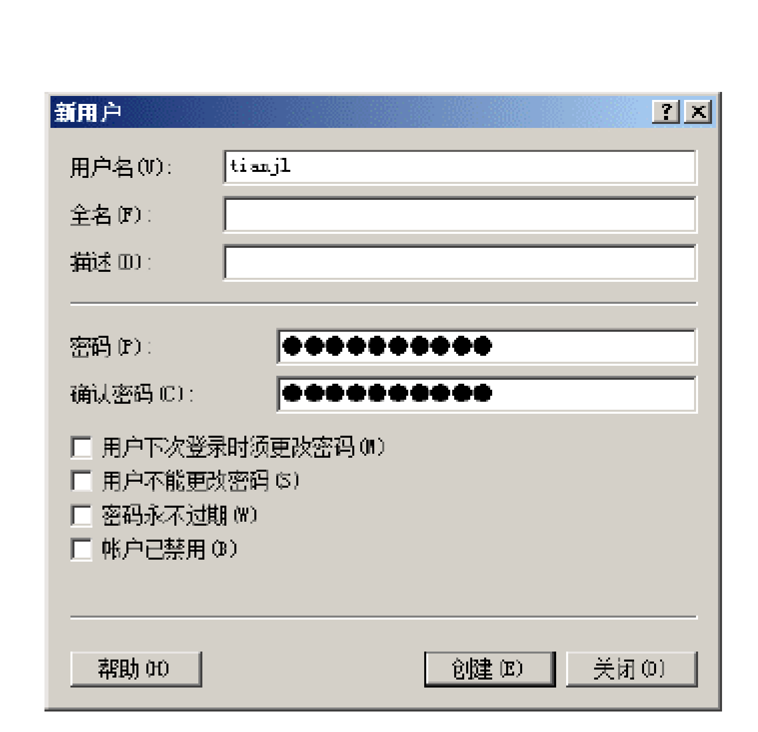


图 5-2 “新用户”对话框

图 5-3 “Active Directory 用户和计算机”窗口

② 在右侧窗口空白处右击，选择快捷菜单中的“新建”→“用户”命令，打开如图 5-4 所示的“新建对象 – 用户”对话框，输入新创建的用户的信息。在“姓”文本框中输入新用户的姓氏；在“名”文本框中输入新用户的名称；在“用户登录名”文本框中输入用户用来登录域的账号名；“用户登录名(Windows 2000 以前的版本)”是用户从 Windows 2000 以前的 Windows 系统登录域时使用的用户名，保持默认即可。



提示： 建议管理员在创建用户账户时，尽量输入详细的用户信息，便于日后维护和安全管理工作。

③ 单击“下一步”按钮，显示如图 5-5 所示的对话框，为新添加的用户指定登录域时使用的密码，并指定对于密码的控制权限。操作方法与在本地计算机上创建用户账户时完全相同，此处不复赘述。



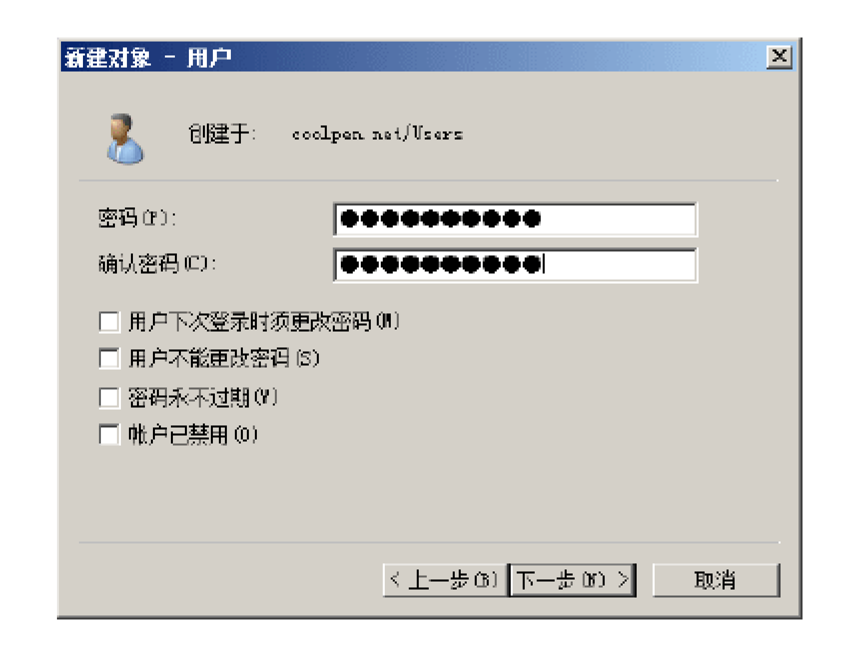
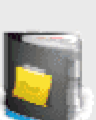


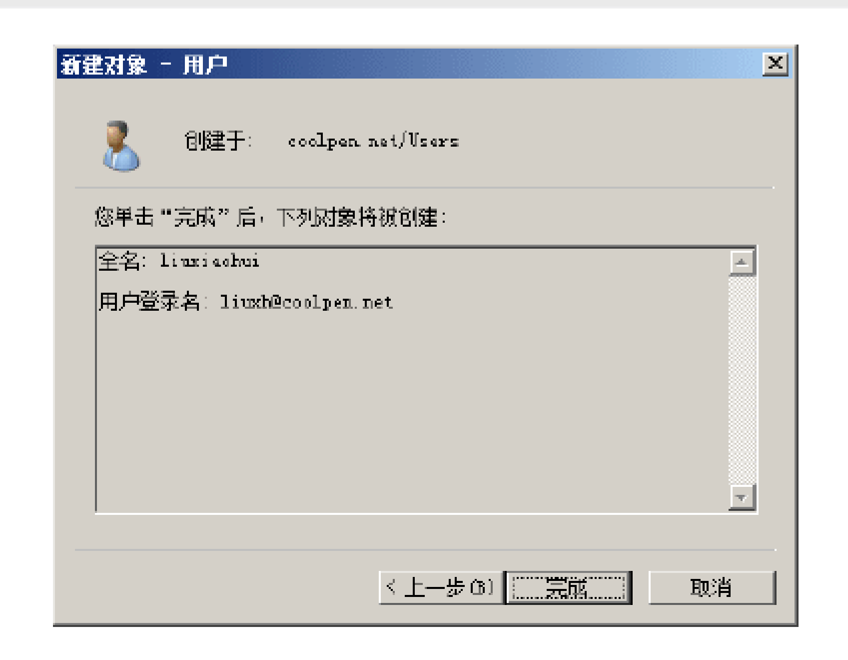

图 5-4 “新建对象 – 用户”对话框

图 5-5 设置用户账户密码


提示：为了提高网络的安全性，对所有账户密码的设置，应尽量使用含字母、数字及下划线随机组合的密码，密码之间尽量不相关，以确保账户的安全。

④ 单击“下一步”按钮，显示如图 5-6 所示的用户信息摘要对话框，单击“完成”按钮，即可完成新用户的创建。

注意：如果设置的密码不符合 Windows Server 2008 网络系统密码规则，将提示如图 5-7 所示的“Active Directory 域服务”对话框，返回重新更改即可。



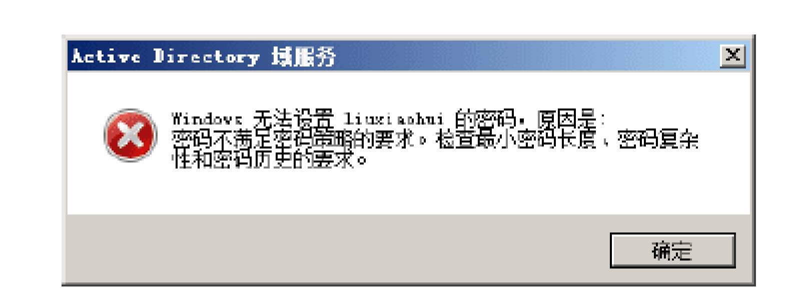


图 5-6 确认新用户信息

图 5-7 “Active Directory 域服务”对话框

5.1.2 重设用户密码

密码是用户登录系统和网络的唯一凭证，如果丢失密码就无法登录。为了确保用户可以继续使用原账户，管理员必须为其重新设置密码。另外，即使没有丢失密码，也应定期更换不同的密码，以免因密码使用时间过长而被别人窃取。

1. 设置本地用户密码

默认情况下，本地计算机的系统管理员账户可以随时通过“计算机管理”工具更改所有用户账户的登录密码。而其他用户则无此权限，只能通过更改密码向导实现。

(1) 管理员账户重设普通账户密码

① 打开“计算机管理”窗口，展开“本地用户和组”→“用户”，右击需要更改密码的用户账户，选择快捷菜单中的“设置密码”命令，显示如图 5-8 所示的“为 hstjl 设置密码”对话框。

② 单击“继续”按钮，显示如图 5-9 所示的对话框，在“新密码”和“确认密码”文本框中输入新密码。由于用户加密文件和个人安全证书中都包含有原来的密码信息，更改后将无法访问这些加密文件并失去个人安全证书的访问权。除非用户账户密码丢失，建议管理员慎重使用该方式为成员用户重设密码。

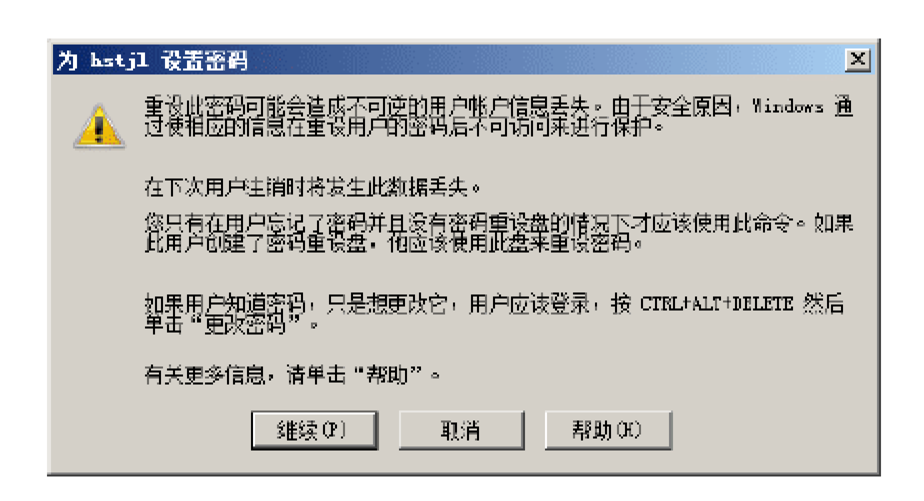


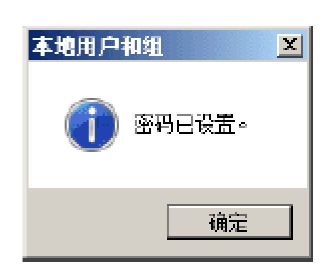
图 5-8　“为 hstjl 设置密码”对话框

图 5-9　输入新密码对话框

③ 单击“确定”按钮，显示如图 5-10 所示的“本地用户和组”对话框。



提示：默认情况下，普通用户账户禁止通过这种方式更改自己的密码，操作时会提示如图 5-11 所示的对话框。通过修改本地组策略设置，可以取消这种限制，不过为确保系统安全，建议不要更改。



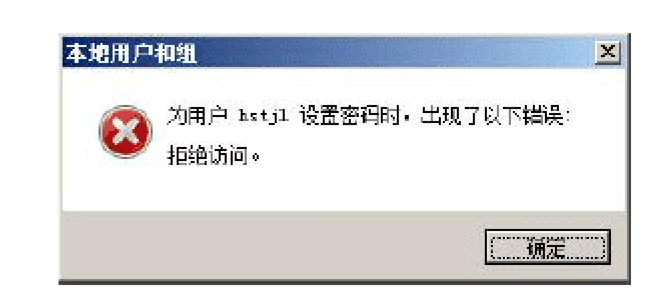




图 5-10　“本地用户和组”对话框　　图 5-11　拒绝访问

(2) 普通账户重设自己密码

① 登录想要更改密码的用户账户，按 Ctrl+Alt+Del 组合键打开如图 5-12 所示的窗口，该窗口类似于 Windows Server 2003 系统的“Windows 安全”窗口。

② 单击“更改密码”按钮，打开如图 5-13 所示的对话框，只有正确输入旧密码后，新密码才可以生效。在“旧密码”文本框中输入用户账户的当前密码，在“新密码”和“确认密码”文本框中输入新的密码即可。

③ 单击“确定”按钮，修改成功，显示如图 5-14 所示的对话框。



提示：Windows Server 2008 对更改密码的要求非常严格，如果不符合密码策略中的任何一项限制，都会出现如图 5-15 所示的对话框。默认情况下密码策略要求如下:

- 密码必须符合复杂性要求。
- 密码长度至少为 7 个字符。
- 密码最短使用时间为 1 天。
- 密码最常使用期限为 42 天。
- 不得使用历史密码，默认记录 24 个历史密码。



图 5-12　Windows 安全窗口

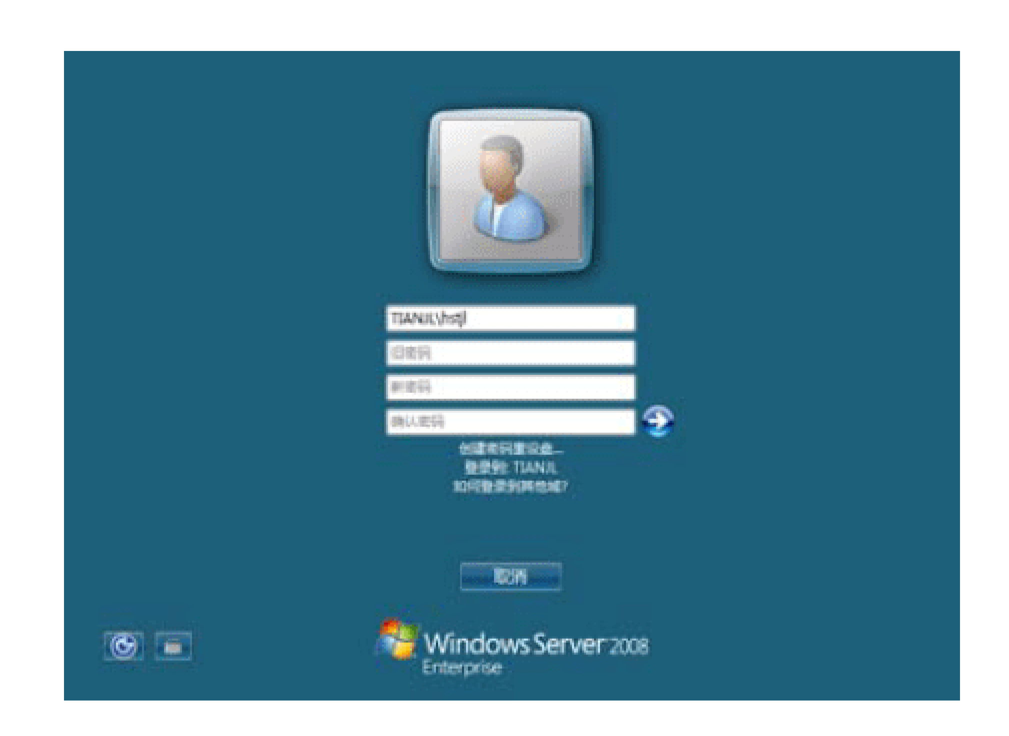


图 5-13　更改密码



图 5-14　修改密码成功



图 5-15　新密码不符合要求

④　单击“确定”按钮，返回 Windows 资源管理器。

(3)　创建密码重置盘

“创建密码重置盘”是确保账户密码安全的重要手段，创建过程中会将用户账户和密码信息，以加密的方式存储到指定的软盘或 U 盘上。忘记登录密码时，使用这些信息可以重新创建一个新的安全密码，实现登录系统的目的。

①　在“更改密码”窗口中，单击“创建密码重置盘”链接，启动“忘记密码向导”，显示如图 5-16 所示的“忘记密码向导”对话框。

②　单击“下一步”按钮，显示如图 5-17 所示的“创建密码重置盘”界面，在“我想在下面的驱动器中创建一个密码密钥盘”的下拉列表框中选择目标盘，软盘或可移动磁盘都可以作为目标盘，用户可以根据自己的实际情况选择。

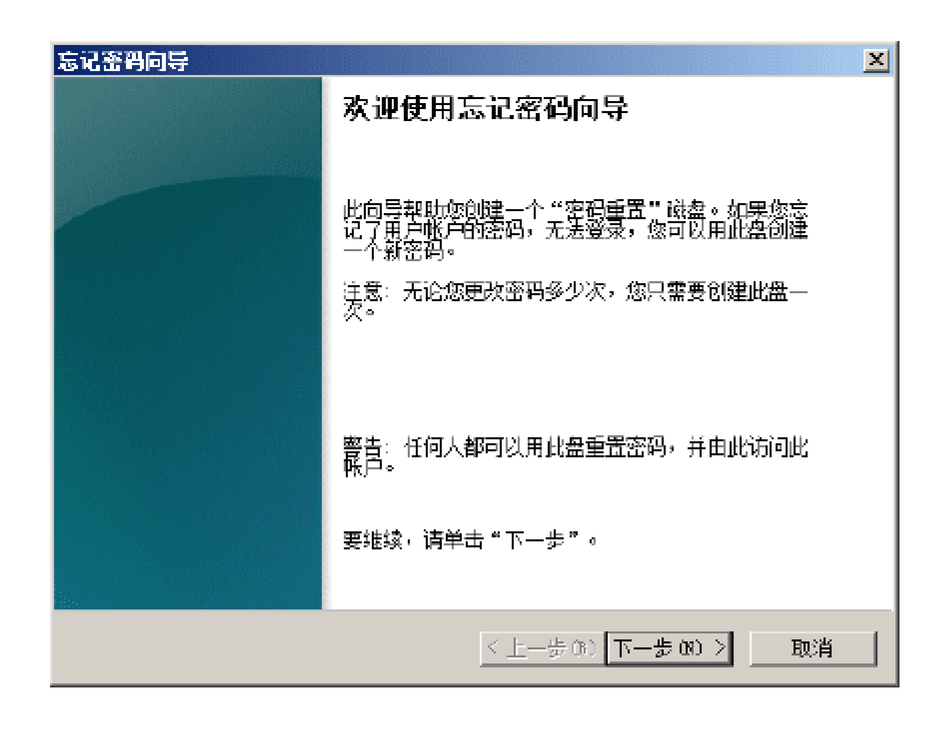


图 5-16　“忘记密码向导”对话框

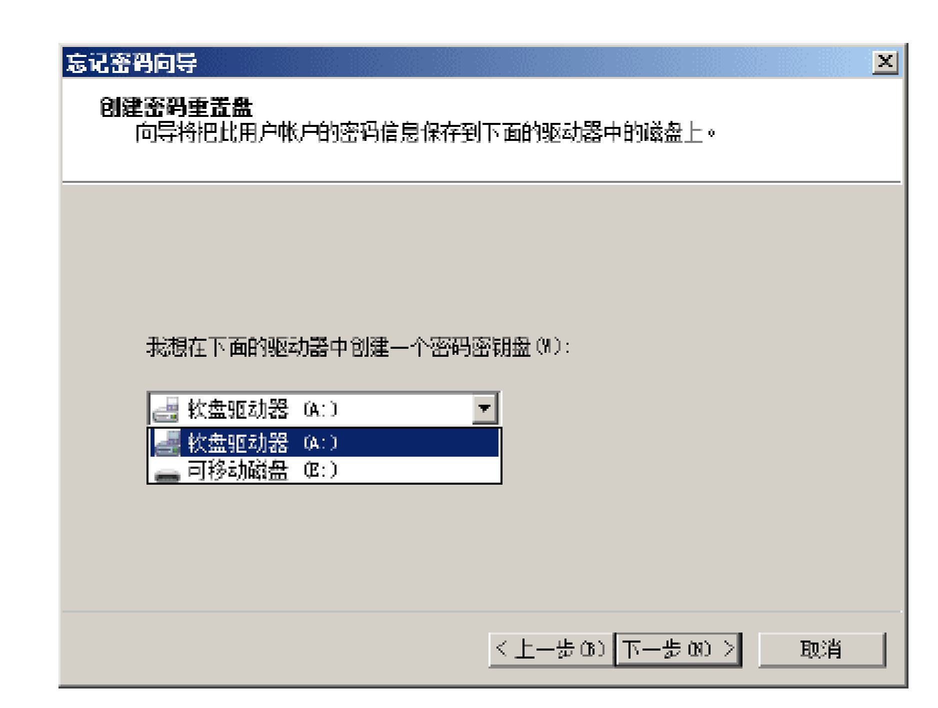


图 5-17　“创建密码重置盘”界面

③　单击“下一步”按钮，显示如图 5-18 所示的“当前用户账户密码”界面。当前用户账户密码为空，所以这里无需输入任何信息。如果为已经设置密码的用户账户创建密码重置盘，则需要输入当前使用的密码。

④　单击“下一步”按钮，开始创建。完成后继续单击“下一步”按钮，显示如图 5-19 所示的“正在完成忘记密码向导”界面。任何人都可以通过密码重置盘，重新设置当前用户账户的密码，因此应做好标记，并妥善保管。

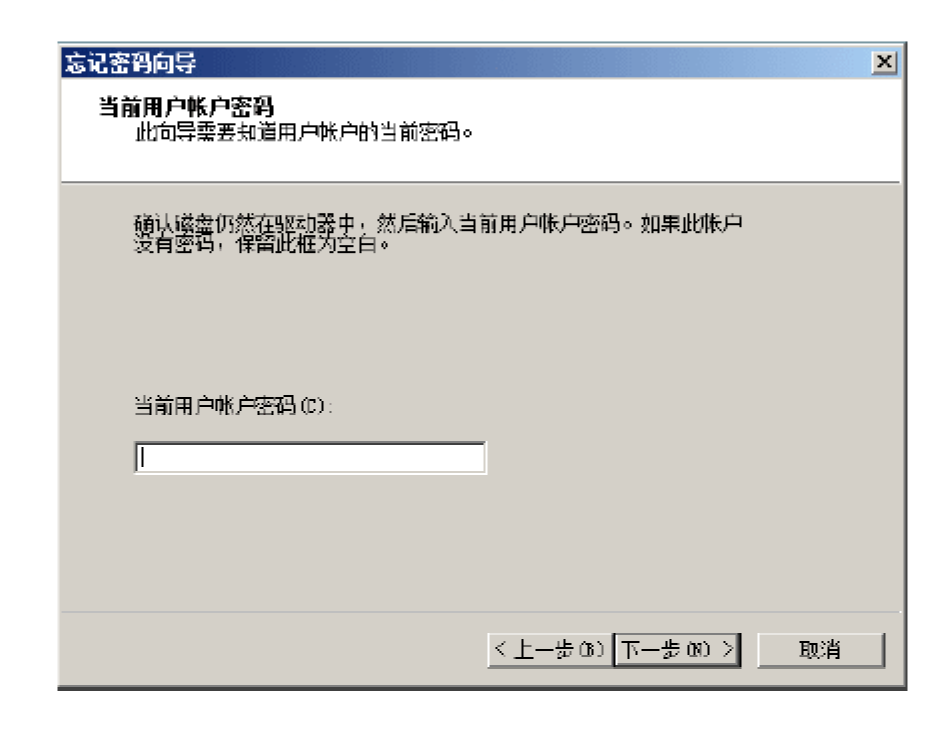


图 5-18　“当前用户账户密码”界面

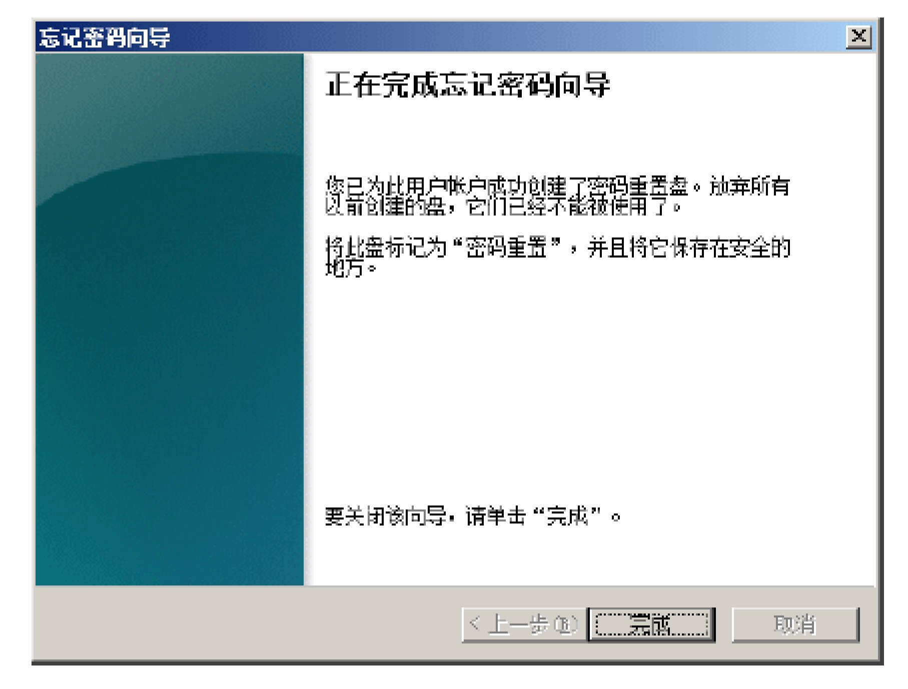


图 5-19　“正在完成忘记密码向导”界面

⑤　单击“完成”按钮，退出向导并返回登录界面。

如果忘记此用户账户的密码，可以在登录界面中选择用户账户后，单击“重设密码”链接启动“重置密码向导”，根据提示信息插入密码重置盘，当运行至如图 5-20 所示的“重置用户账户密码”步骤时，重新设置新的密码即可，此时还可以设置一个密码提示信息。

2. 设置域用户账户密码

在域环境中重设账户密码比较简单。使用具有相关权限的管理员账户登录到域控制器，打开“Active Directory 用户和计算机”窗口。在 Users 容器中，右击想要重置密码的用户账户，选择快捷菜单中的“重置密码”命令，显示如图 5-21 所示的“重置密码”对话框，在“新密码”和“确认密码”文本框中输入新密码，单击“确定”按钮即可。使用这种方法，也可以重设管理员账户的密码。

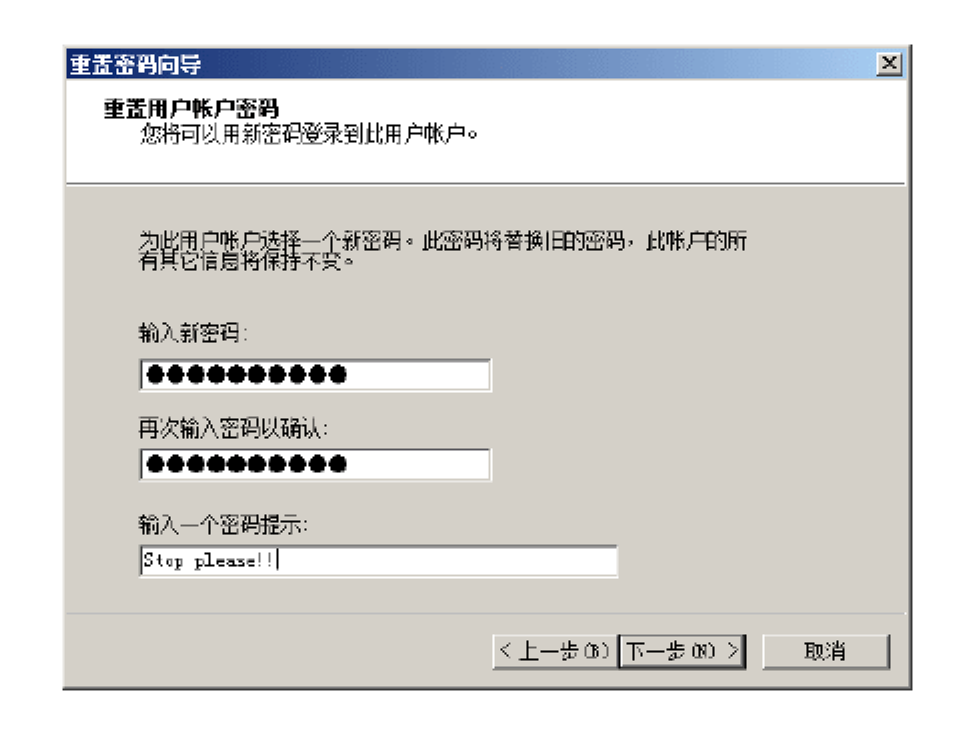


图 5-20　“重置用户账户密码”界面

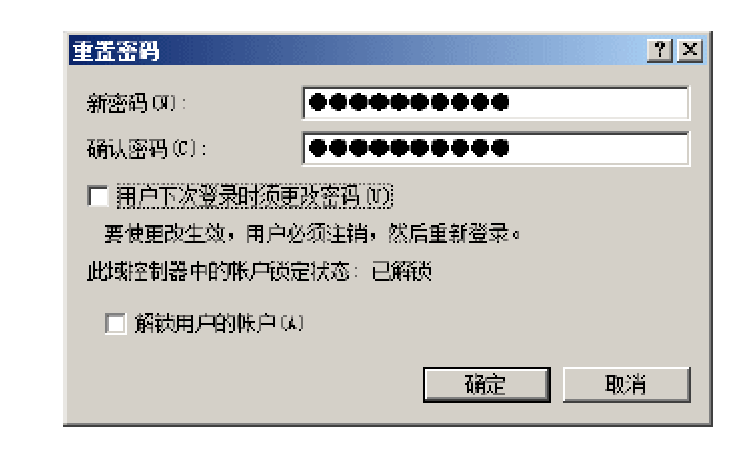


图 5-21　“重置密码”对话框



提示：如果当前账户已被锁定，则可以选中“解锁用户的账户”复选框，使密码更改立即生效。系统默认配置的安全策略可能会限制用户更改密码的次数或登录次数限制，如果超出策略限制，则立即锁定账户，并等待一定时间后自动解锁。此时，对应用户可以告知管理员，由管理员登录到域控制器，使用此方式为其重设密码并解锁账户。

5.1.3 启用、禁用、删除用户

账户和用户是相互对应的。如果新用户加入，需要创建新的账户；如果有些账户临时不用，则可以暂时将其禁用，以免被其他用户滥用；如果用户完全脱离计算机或域，则可以删除对应账户。每个用户账户都可能对系统安全造成威胁，通常情况下只保留够用的账户即可。

1. 禁用、启用和删除本地用户账户

以具有管理员权限的账户登录系统，打开“计算机管理”的“用户”窗口，双击需要禁用的用户账户，打开用户账户的属性对话框，在“常规”选项卡中，选中“账户已禁用”复选框，如图 5-22 所示。单击“确定”按钮即可禁用该账户。取消选中“账户已禁用”复选框，即可重新启用已禁用的账户。



提示：除非有特殊应用，Guest 账户应当被禁用。事实上，许多网络攻击就是借助 Guest 用户来实现的。即使启用 Guest 账户，也应当为其指定最低的访问权限。

在“计算机管理”窗口中，右击需要删除的账户，选择“删除”命令，显示如图 5-23 所示的“本地用户和组”对话框，单击“是”按钮，即可删除所选账户。

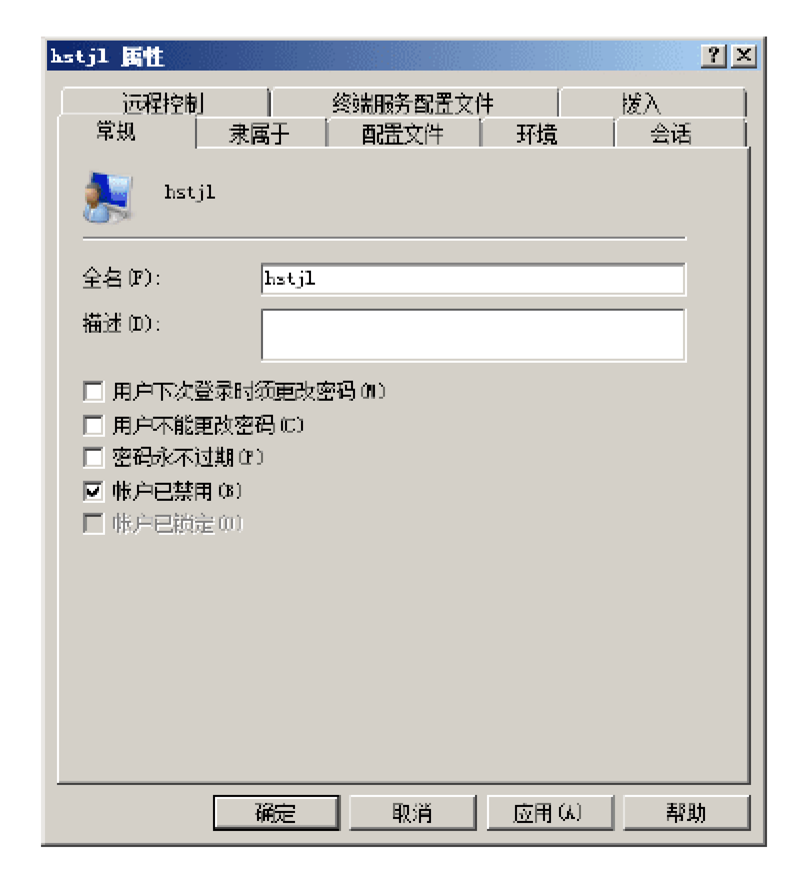


图 5-22 禁用本地用户账户

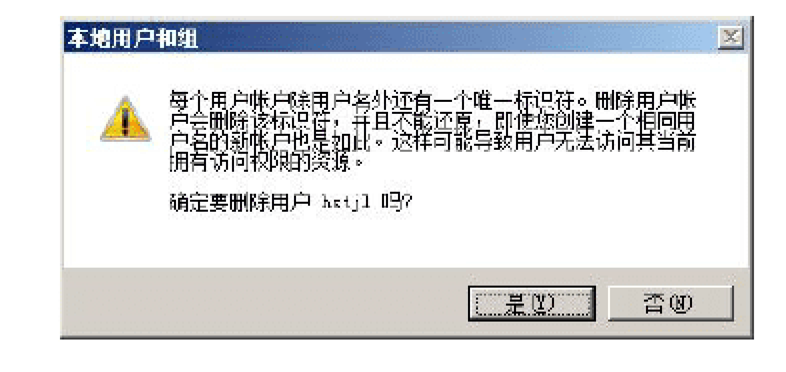


图 5-23 “本地用户和组”对话框

2. 禁用、启用和删除域用户账户

以具有管理员权限的账户登录域控制器，打开“Active Directory 用户和计算机”窗口，右击想要禁用的用户账户，选择快捷菜单中的“禁用账户”命令即可将其禁用，如图 5-24 所示。

用户账户被禁用以后，便不能再登录。如果想启用用户账户，则可以按照相同的方法，选择快捷菜单中的“启用账户”命令即可。如果账户不再使用，或需要重设所有权限，可将其删除，右击用户账户名，

并选择快捷菜单中的“删除”命令即可删除该账户。

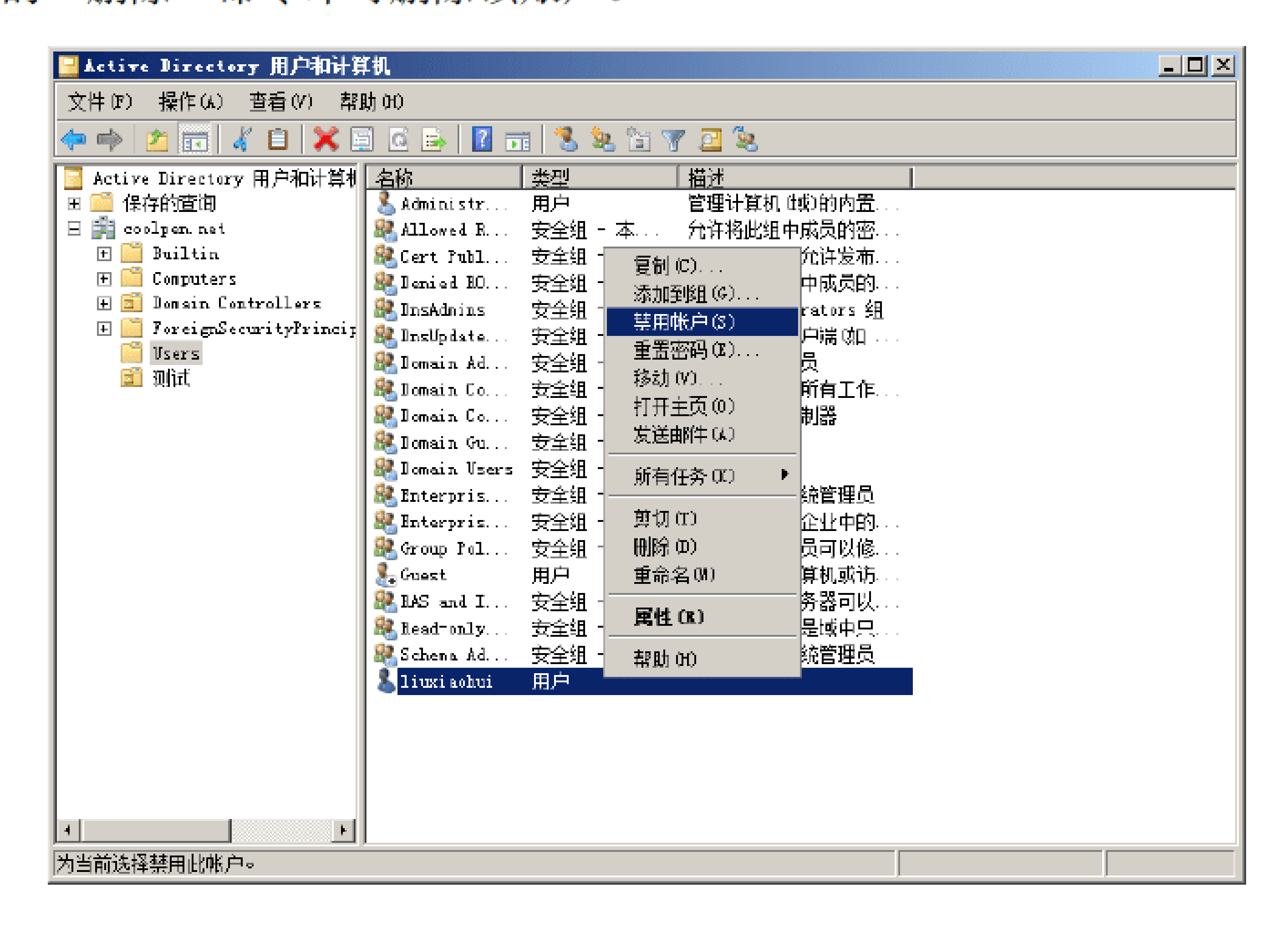


图 5-24 禁用域用户账户

5.1.4 限制用户可以登录的时间

默认情况下，域用户账户可以随时登录到域控制器，但是为了确保服务器系统以及网络的安全，应对用户账户的登录时间进行限制。该限制仅适用于域用户账户，本地用户账户登录系统时间无法限制。

① 在“Active Directory 用户和计算机”窗口中，双击要设置的用户，打开用户属性对话框，如图 5-25 所示。

② 单击“登录时间”按钮，显示如图 5-26 所示的“liuxiaohui 的登录时间”对话框，默认允许在任何时间登录。

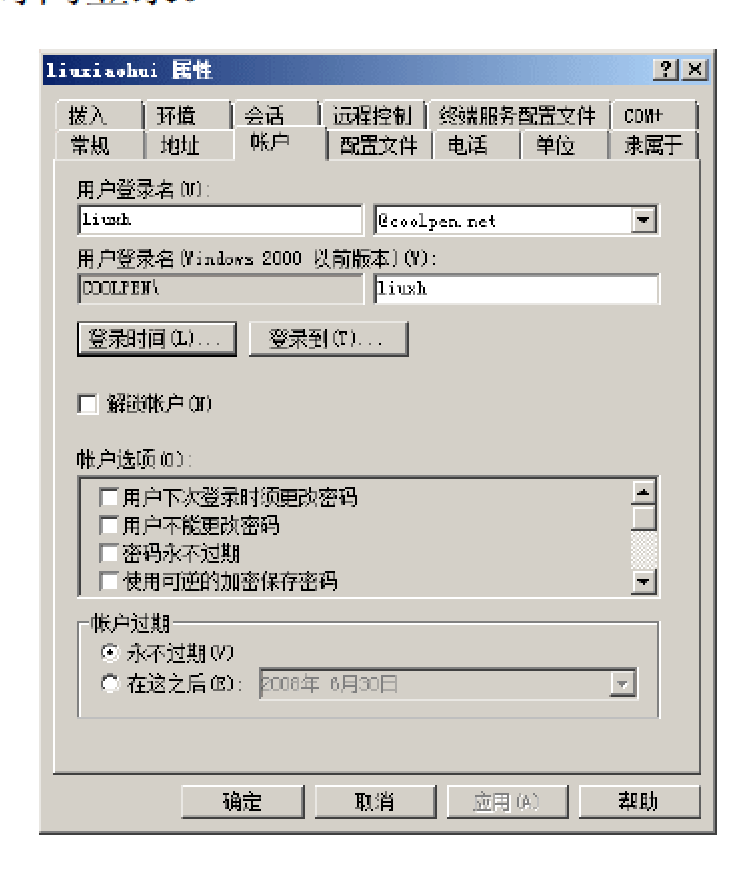


图 5-25 “liuxiaohui 属性”对话框

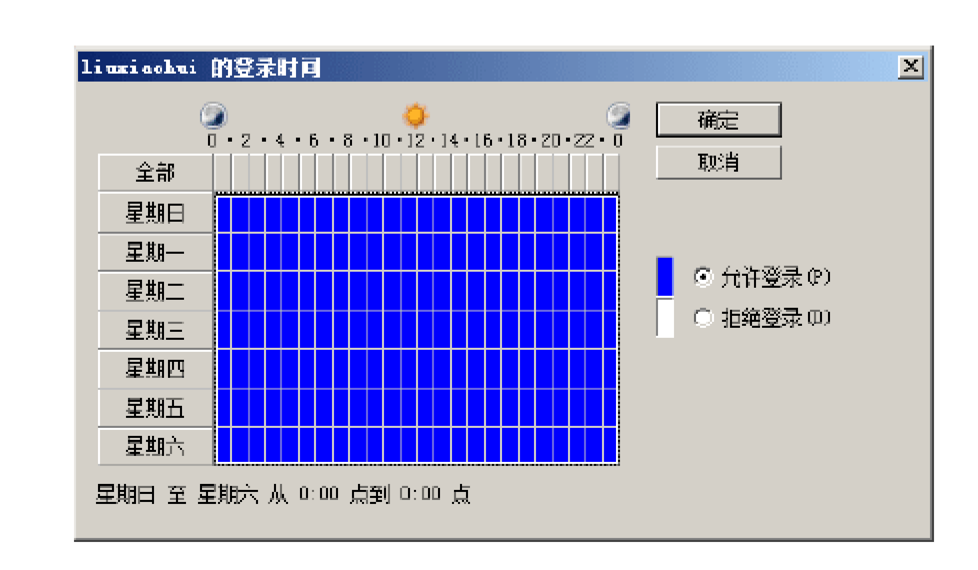


图 5-26 “liuxiaohui 的登录时间”对话框

③ 在登录时间分布表中，框选拒绝登录的时间范围，选择“拒绝登录”单选按钮，如图 5-27 所示。例如，本例中设置的是 liuxiaohui 账户，允许其在每周星期一到星期五的 9 点至 17 点登录域控制器。

④ 单击“确定”按钮保存设置。

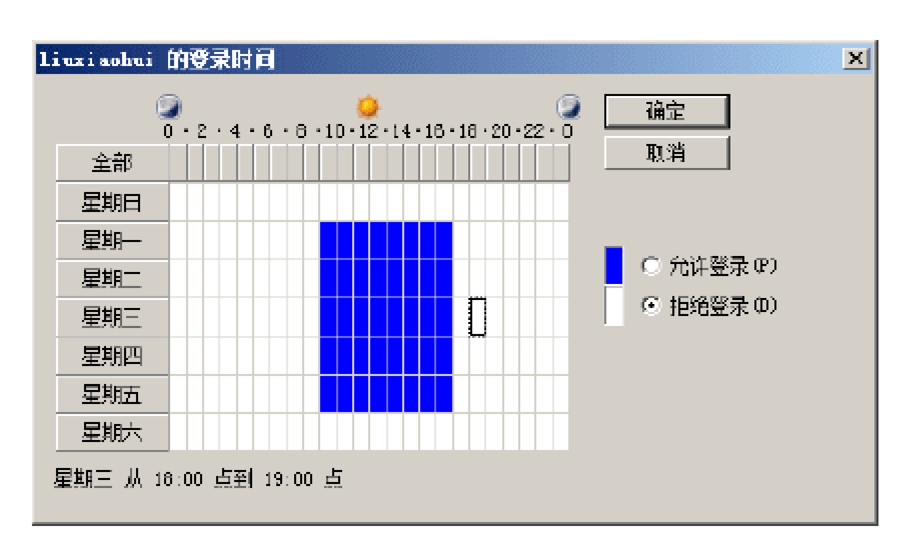


图 5-27　设置登录时间

5.1.5　限制用户可以登录的工作站

限制用户登录到的工作站是指限制用户账户只能从网络中指定的计算机上登录，访问 Active Directory 中的资源。默认情况下，域用户账户可以从网络中任意计算机上登录，通过将用户账户和登录计算机捆绑在一起，可以实施更加有效的安全管理措施。

① 仍然以 liuxiaohui 账户为例，在“liuxiaohui 属性”对话框的“账户”选项卡中，单击“登录到”按钮，显示如图 5-28 所示的“登录工作站”对话框。默认选中“所有计算机”单选按钮，即允许用户登录网络中的所有计算机。

② 选择“下列计算机”单选按钮，在“计算机名称”文本框中输入允许登录的工作站的 NetBIOS 名称，单击“添加”按钮添加到列表中，可以添加多个允许登录的工作站名称。

③ 单击“确定”按钮保存设置。

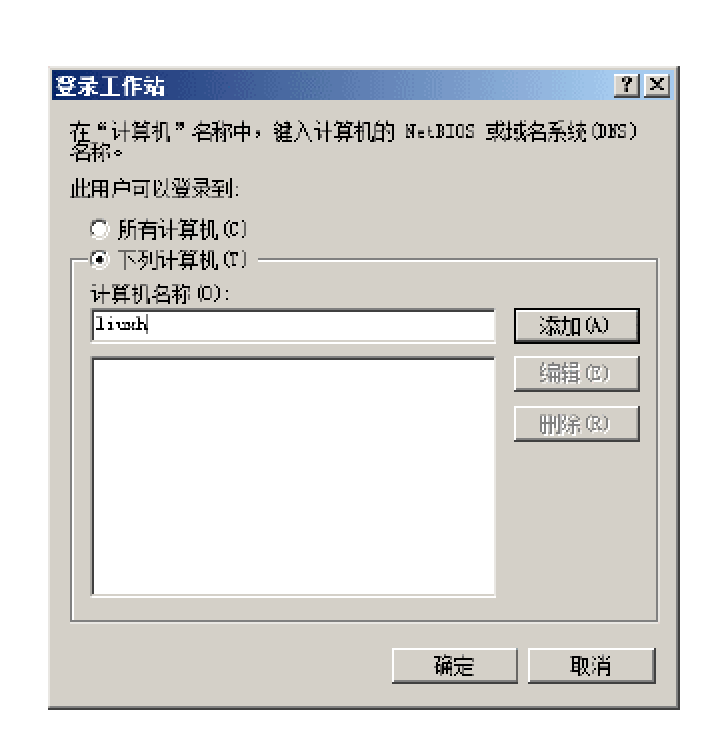


图 5-28　“登录工作站”对话框

5.1.6　恢复误删除的域用户

在 Windows Server 2008 的“Active Directory 用户和计算机”管理控制台中，没有提供对误删除的用户恢复的功能。管理员可以借助 Adrestore.exe 工具，在命令行模式下恢复误删除的用户，该工具支持 Windows 2000 Server/ Windows Server 2003/ Windows Server 2008 系统中的活动目录。本例以恢复被删除的“Testuser”用户为例，介绍用 Adrestore.exe 工具恢复用户的方法。

① 将该工具复制到运行 AD DS 域服务的计算机中，选择“开始”→“所有程序”→“附件”→“命令提示符”命令，显示如图 5-29 所示的命令提示符窗口，并切换到存储 Adrestore.exe 工具的文件夹中。

② 在命令行提示符下，输入如下命令：

```
Adrestore /r
```

按 Enter 键，命令成功执行，显示如图 5-30 所示的窗口，该命令枚举活动目录中删除的对象，并显示用户完整的 FQDN(Fully Qualified Domain Name，完全合格域名)信息。

③ 输入“Y”，恢复删除的用户信息，提示用户被成功恢复，如图 5-31 所示。用同样的方法可以恢复其他被删除的 Active Directory 对象。



图 5-29　切换到“Adrestore.exe”工具所在的目录

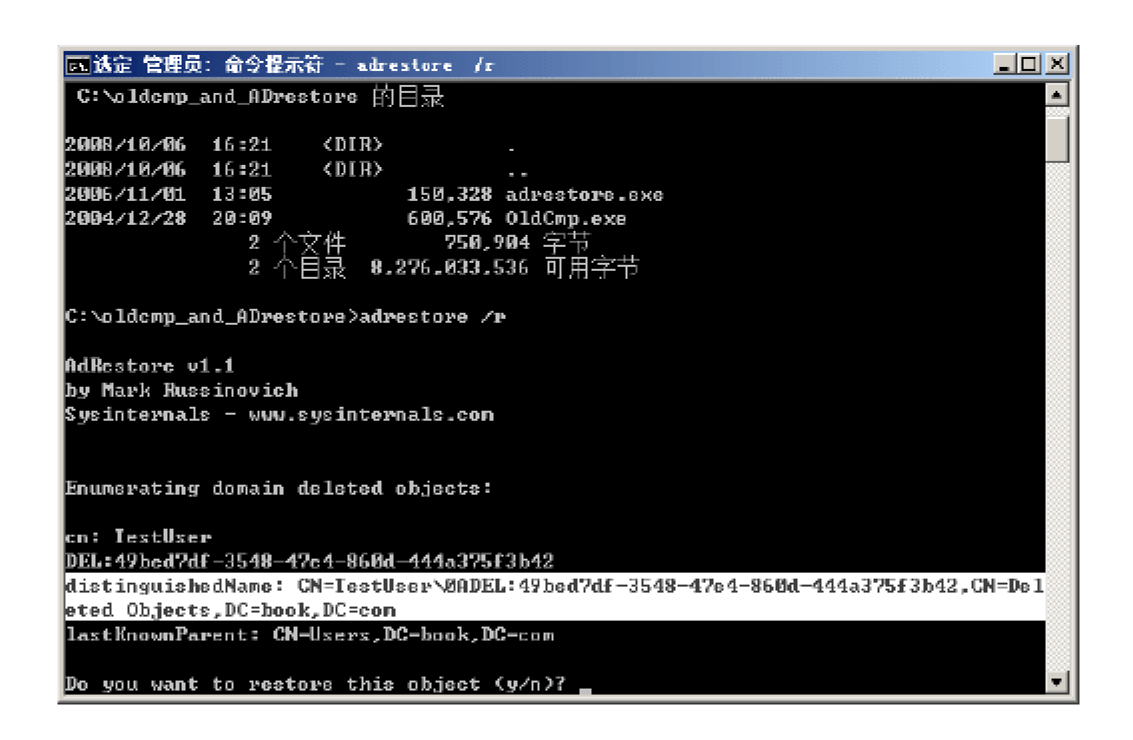


图 5-30　枚举活动目录中被删除的对象

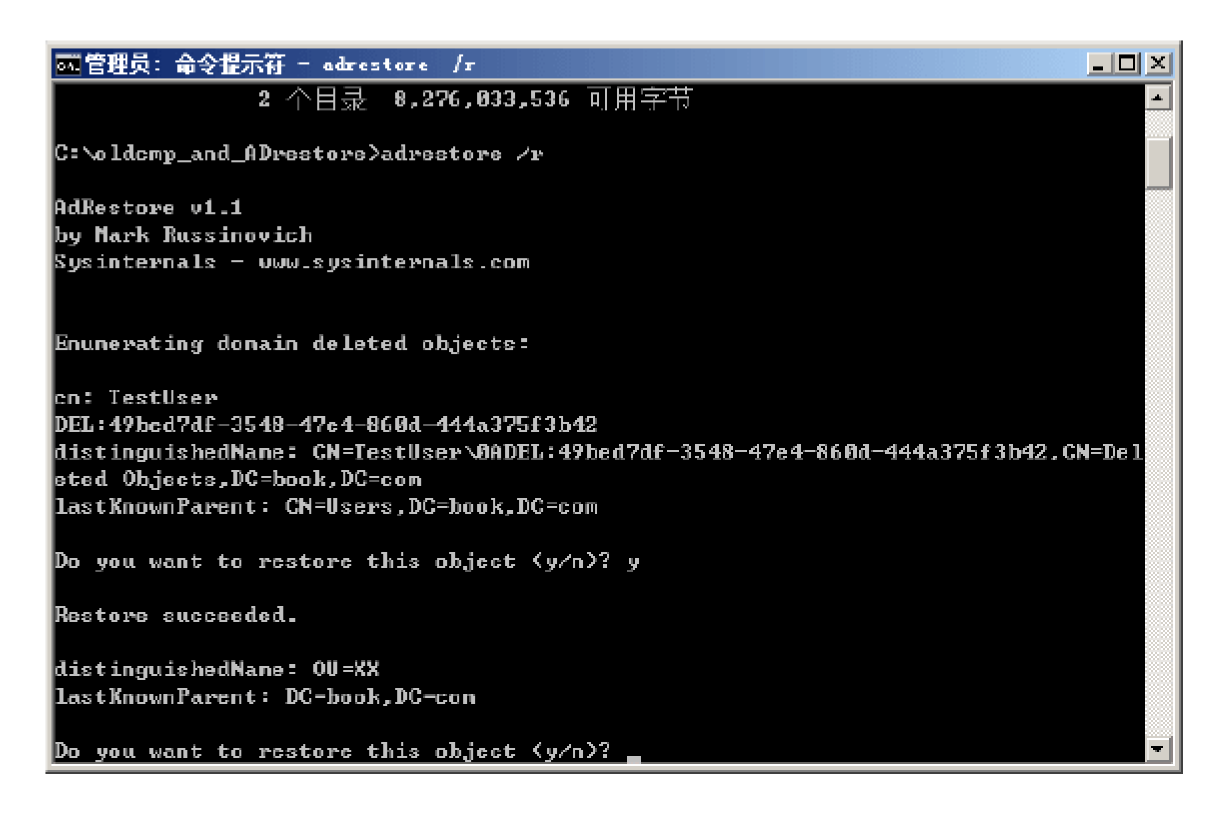


图 5-31　恢复误删除的用户

④　打开“Active Directory 用户和计算机”窗口，选择“Active Directory 用户和计算机”→book.com→Users 选项，在右侧窗格中 TestUser 被成功恢复，恢复的用户状态为“禁用”，如图 5-32 所示。

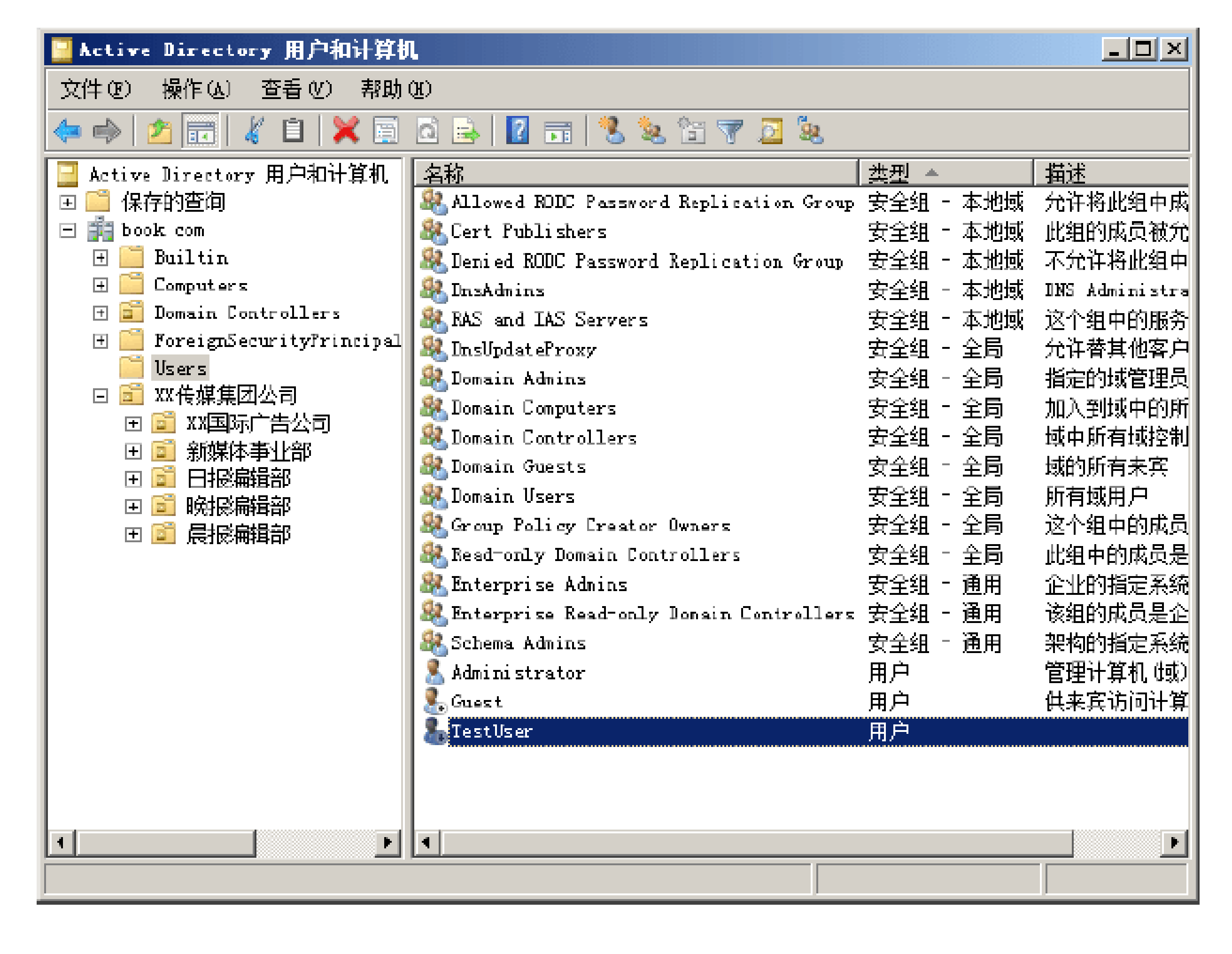


图 5-32　被删除用户已被恢复

⑤ 恢复的账户需要重新设置密码，启用该账户即可完整恢复被删除的用户账户。

5.2 用户组的管理

用户组是常用组的一种，尤其是在域环境中，应用更多。在稍具规模的域网络中，就可能存在成百上千的用户账户，如果逐个为每个账户设置权限，显然非常麻烦，而且容易出错。借助用户组，可以将希望赋予相同权限的用户账户添加到同一组中，只需为该组设置权限，即可应用到每个用户账户。为了减轻管理员的工作负担，还可以在用户组中指定组管理员，完成组中成员的常规管理工作。

5.2.1 新建用户组

默认情况下，系统安装完成后，已经自动创建了一些默认用户组，需要注意的是，这些用户组往往用于实现特殊的系统管理任务，不可随意更改其中的成员和属性信息。在日常应用中，管理员可以随意创建用户组，用于存储指定类型的用户账户。如果是在域环境中，管理员还可以通过设置组的作用域，决定其中成员在域中的应用领域。

1. 创建本地用户组

对于独立服务器而言，用户组的作用并不大，但为了实现对用户账户的统一管理，也可以创建所需的本地用户组。

① 以具有管理员权限的账户登录系统，打开“计算机管理”控制台，依次选择“本地用户和组”→“组”选项，在右侧窗格中列出了所有的组，如图 5-33 所示。

② 右击“组”并选择快捷菜单中的“新建组”命令，显示如图 5-34 所示的“新建组”对话框。在“组名”文本框中输入新组的名称，如果用户组较多，还可以输入适当的描述信息，以便区分。

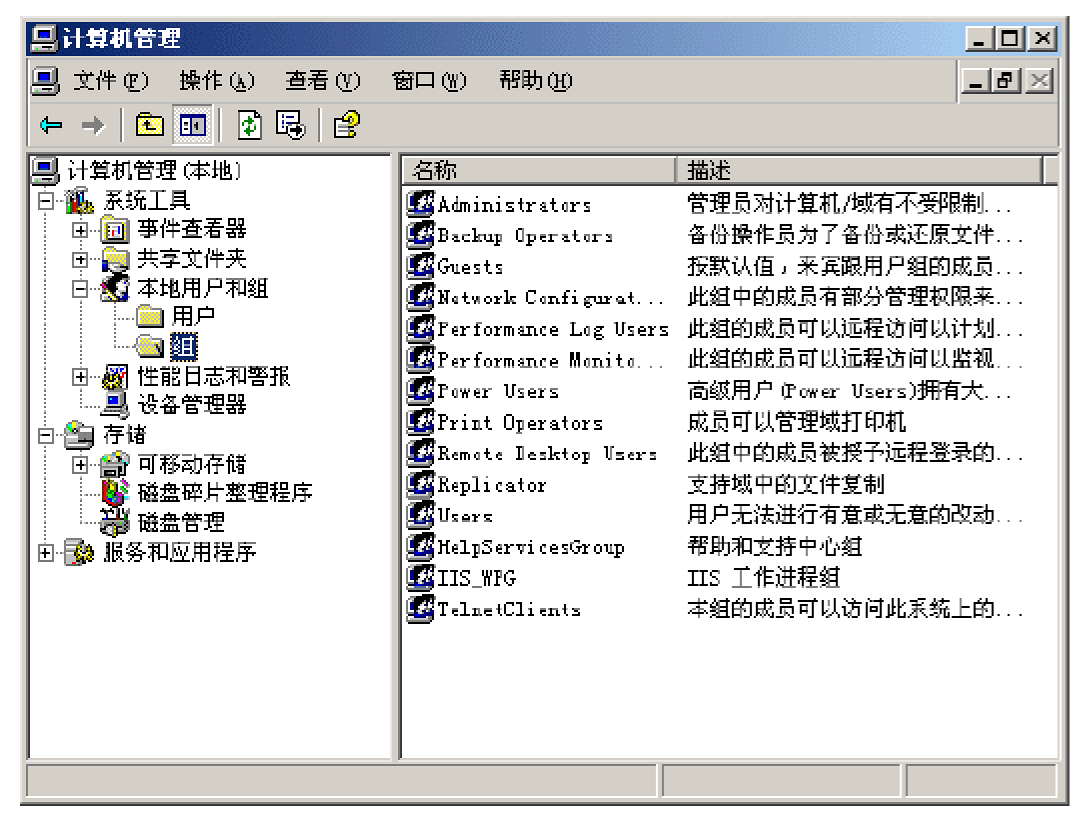


图 5-33 所有本地用户组

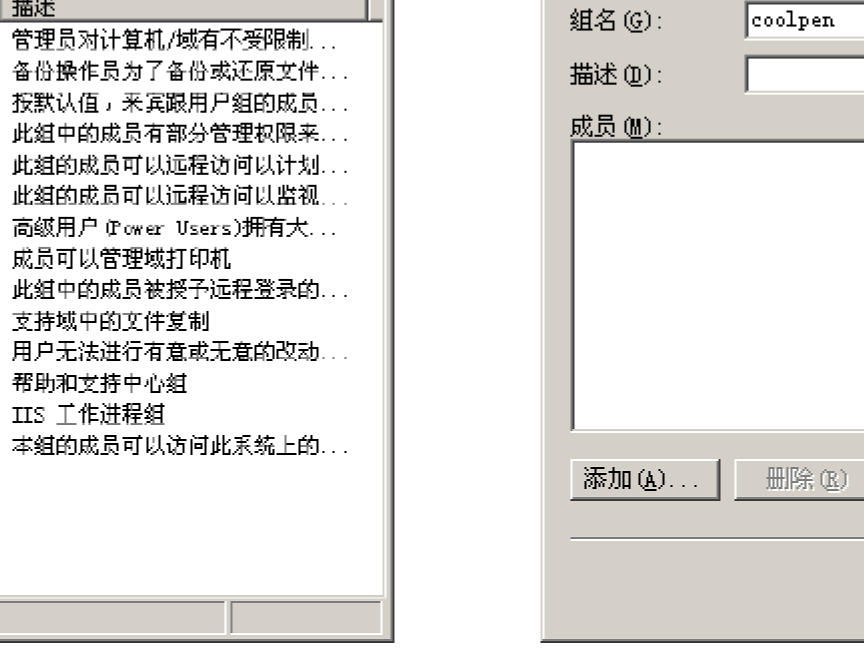


图 5-34 “新建组”对话框

③ 单击“添加”按钮，显示如图 5-35 所示的“选择用户”对话框，在“输入对象名称来选择”文本框中，输入要添加到新组的用户账户名，单击“确定”按钮添加到该组。

④ 单击“创建”按钮，新组创建完成。如果不希望立即添加组成员，也可以跳过步骤③操作。

2. 创建域用户账户

在域中，只有拥有管理员权限，或者被委派了相关权限的用户账户，才可以登录到域控制器创建组。

① 打开“Active Directory 用户和计算机”窗口，选择新建组所在的 OU 或容器，如图 5-36 所示。

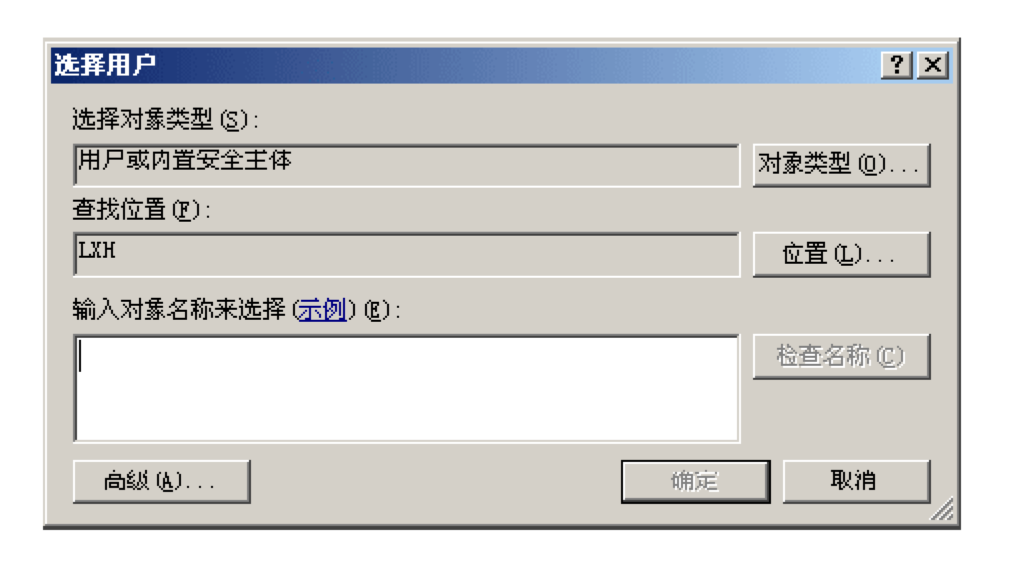




图 5-35　“选择用户”对话框

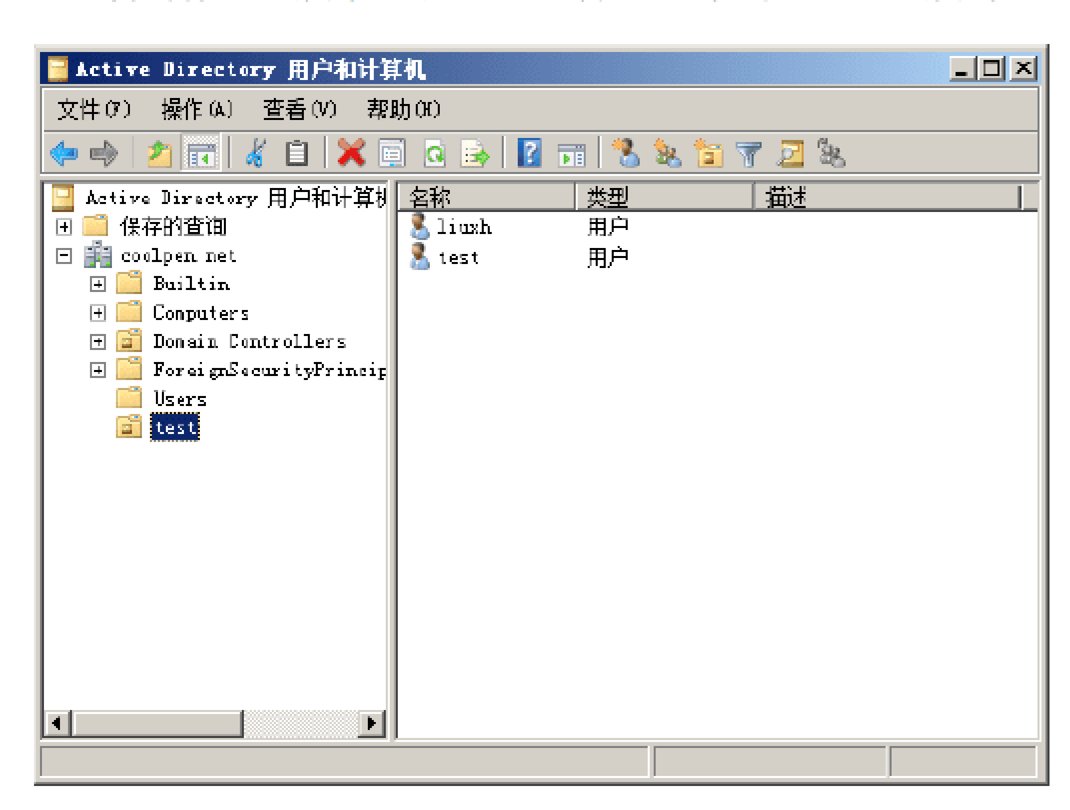


图 5-36　“Active Directory 用户和计算机”窗口

② 在窗口空白处右击，选择快捷菜单中的“新建”→“组”命令，显示如图 5-37 所示的“新建对象 – 组”对话框。在“组名”文本框中，输入需要新建组的名称，如 student；在“组名(Windows 2000 以前版本)”文本框中，系统自动填写对应的组名；在“组作用域”选项区域中选择“全局”单选按钮；在“组类型”选项区域中选择“安全组”单选按钮。

③ 单击“确定”按钮，完成安全用户组的创建。



图 5-37　“新建对象 – 组”对话框

5.2.2　向组中添加成员

在创建本地用户组过程中，即可完成用户账户的添加。而域用户组则需要创建完成后手动添加。组成员可以包括用户账户、联系人、其他组或计算机。例如，可以将一台计算机加入某组，使该计算机有权访问另一台计算机上的共享资源。

① 以具有管理员权限的用户账户登录到域控制器，打开如图 5-38 所示的“Active Directory 用户和计算机”窗口，找到域管理的用户组所在的组织单位或容器。

② 双击需要添加成员的用户组(以 coolpen 用户组为例)，打开“coolpen 属性”对话框，切换到如图 5-39 所示的“成员”选项卡，“成员”列表框中用来显示该组中所有的成员，默认为空。

③ 单击“添加”按钮，打开“选择用户、联系人、计算机或组”对话框，单击“立即查找”按钮，开始搜索域中的所有用户账户，如图 5-40 所示。

④ 借助于 Ctrl 和 Shift 键，在列表框中选择所有欲添加至该组的用户，单击“确定”按钮，所选择的计算机和用户账户将被添加至该组，并显示在列表框中(如图 5-41 所示)。当然，如果知道用户账户的准确名称，也可以直接在“输入对象名称来选择”文本框中输入账户名，用户之间用“;”分隔开来。

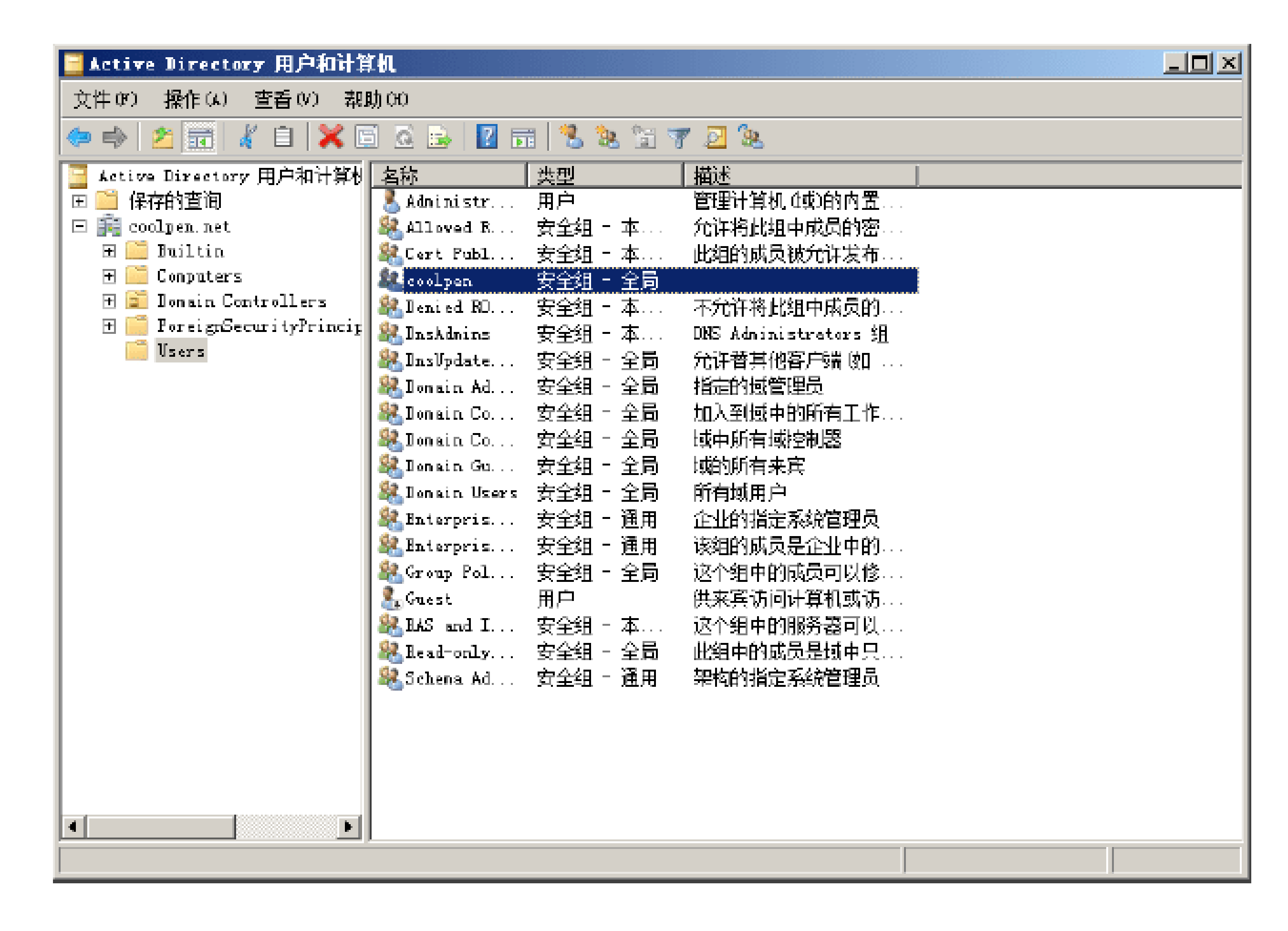


图 5-38 “Active Directory 用户和计算机”窗口

图 5-39 “成员”选项卡

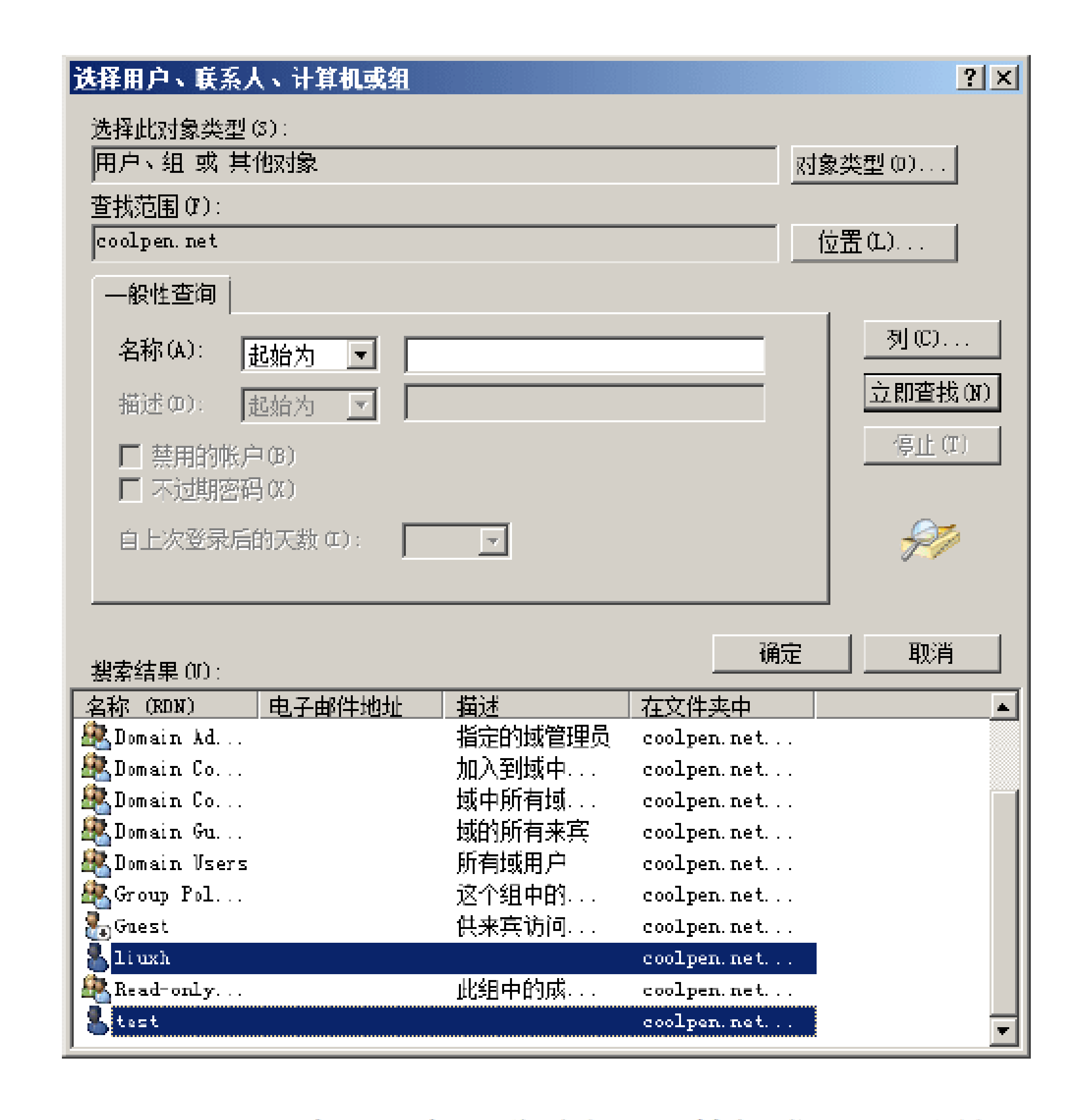


图 5-40 “选择用户、联系人、计算机或组”对话框

图 5-41 所选择的用户账户

⑤ 单击“确定”按钮，返回组属性对话框，所有被选择的计算机和用户账户被添加至该组，如图 5-42 所示。

⑥ 单击“确定”按钮，完成用户的添加。

除通过上述方式添加组成员外，也可以将指定用户账户添加到某个或几个组。在“Active Directory 用户和计算机”窗口中，右击要添加到组的用户账户，选择快捷菜单中的“添加到组”命令，显示如图 5-43 所示的“选择组”对话框，在“输入要选择的对象名称”文本框中输入欲添加到的组，多个组之间需要用“;”隔开。最后，单击“确定”按钮，所选择的用户被添加到组中。




图 5-42　“coolpen 属性”对话框

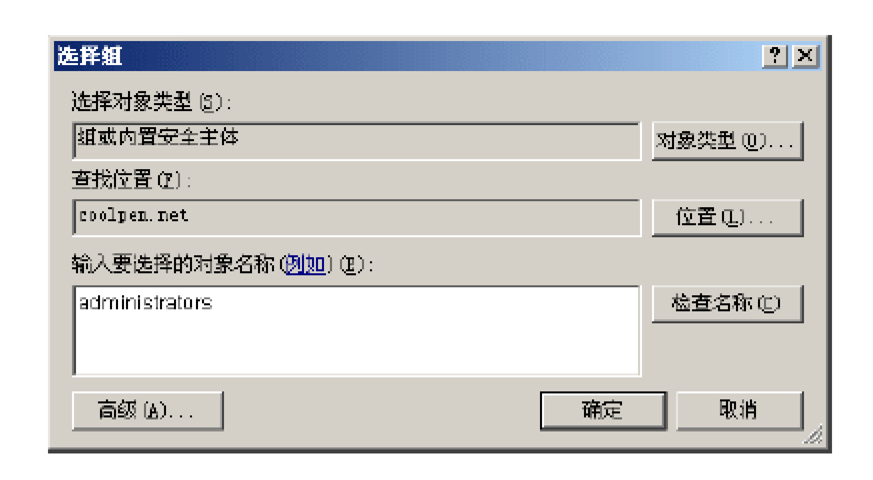


图 5-43　“选择组”对话框

5.2.3　为组指定管理员

组管理员只是针对域用户组而言的，独立服务器不具有此功能。在独立服务器系统中，只有管理员账户可以管理所有用户组，如更新成员列表、更改账户权限等。而在域中，可以为组指定特定的管理者，使其可以完成组中成员的某些工作，如权限委派等。需要注意的是，默认情况下，指定组管理员后，其他任何用户甚至管理员都将无法管理该组。

① 打开“Active Directory 用户和计算机”控制台，选择要指定管理员的组，如 coolpen，右击并选择快捷菜单中的“属性”命令，显示“coolpen 属性”对话框，切换到如图 5-44 所示的“管理者”选项卡。

② 单击“更改”按钮，显示如图 5-45 所示的“选择用户、联系人或组”对话框。在“输入要选择的对象名称”文本框中，输入要指派的管理者的用户名或组名。需要注意的是，这里只能选择一个管理者。

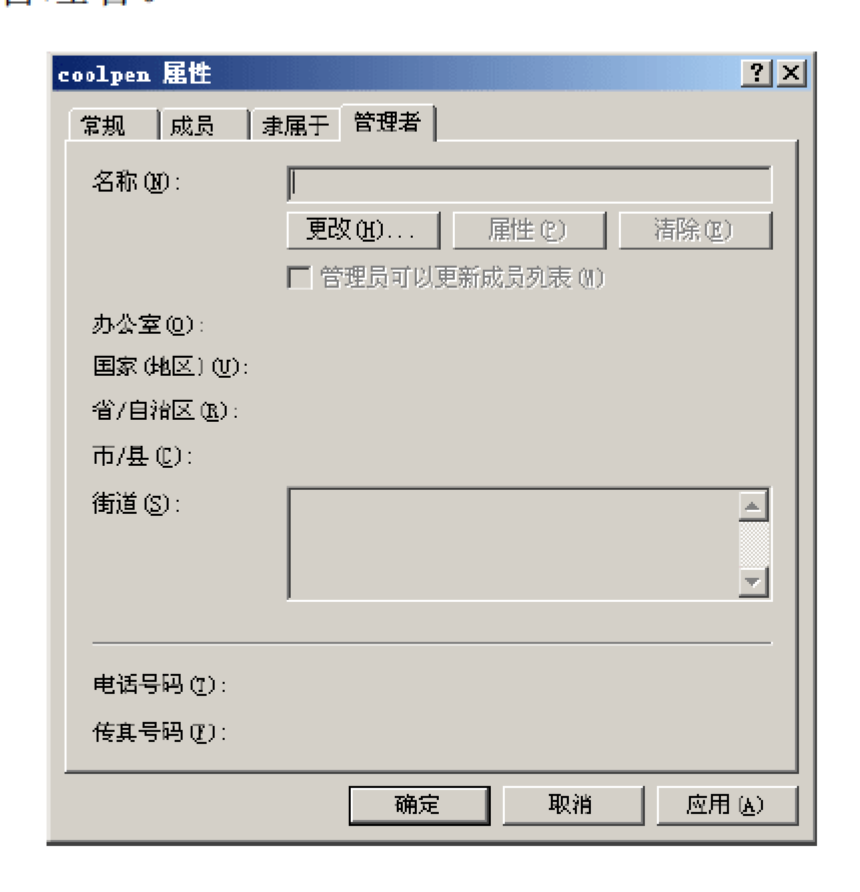


图 5-44　“管理者”选项卡

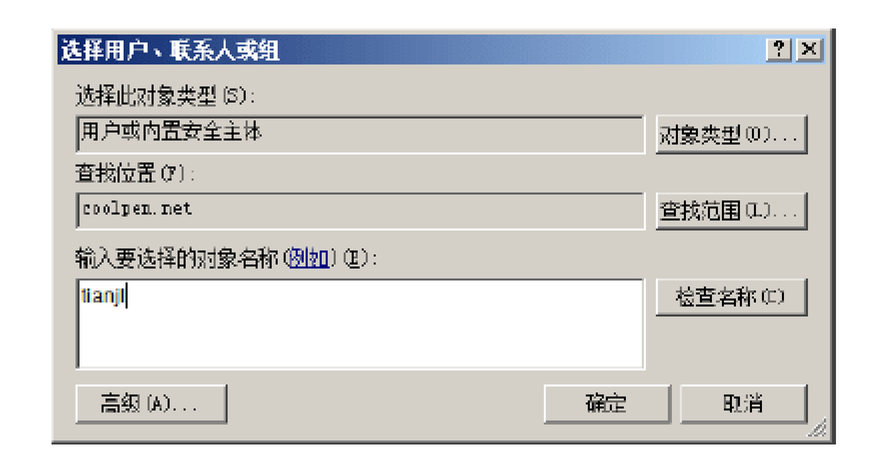


图 5-45　“选择用户、联系人或组”对话框

③ 单击“确定”按钮返回“管理者”选项卡，在“姓名”文本框中，显示了所添加的管理者用户名称，如图 5-46 所示。如果要清除管理者用户账户，单击“清除”按钮即可。

默认情况下，“管理员可以更新成员列表”复选框没有被选中，表示只有被指定的管理者才能管理该组，即使是域管理员也无此权限。如果选中该复选框，则允许管理员账户更新组成员列表。

④ 单击“确定”按钮，完成组的管理者的指派。

图 5-46 已指定管理者

5.2.4 更改组作用域或组类型

1. 组作用域

组的作用域决定了组的作用范围、组中可以拥有的成员以及组之间的嵌套关系。在 Windows Server 2008 域模式下组有 3 种组作用域：通用域、全局和本地域。

- 通用域组的成员：可以包括域树或林中任何域中的其他组和账户，而且可在该域树或林中的任何域中指派权限。
- 全局组的成员：可以包括只在其中定义该组的域中的其他组和账户，而且可在林中的任何域中指派权限。
- 本地域组的成员：可以包括 Windows Server 2008、Windows Server 2003、Windows 2000 Server 或 Windows NT 域中的其他组和账户，而且只能在域内指派权限。

(1) 本地域

具有本地域作用域的组将帮助定义和管理对单个域内资源的访问。这些组可将以下组或账户作为其成员：

- 具有全局作用域的组。
- 具有通用作用域的组。
- 账户。
- 具有本地域作用域的其他组。
- 上面任意组的组合。

(2) 全局

所谓“全局”就是指整个域，此类组属于某个指定域，但作用域却是整个森林。全局组的成员只能是在本地的域中可以访问在森林任何域里的资源。全局组只能放置在同一个域中的资源对象安全描述符中，即不能只是基于另一个域的全局组用户成员身份，而限制对相应对象的访问。在用户登录到一个域时，用户的全局组成员身份将被评估。因为全局组成员身份是以域为中心的，所以全局组成员身份的更改不会强行复制到整个企业范围的全局编录。在“本机模式”域中，全局组可相互嵌套。

管理员只能在创建该全局组的域上进行添加用户账户和全局组，而且全局组可以嵌套在其他组中。可以将某个全局组添加到同一个域上的另一个全局组中，或添加到其他信任域的通用组和域本地组中(不能加入到不同域的全局组中，全局组只能在创建它的域中添加用户和组)。虽然可以利用全局组授予访问任何域上的资源的权限，但一般不直接用它进行权限管理。

(3) 通用域

使用具有通用作用域的组可以合并跨越不同域的组，所以，将账户添加到具有全局作用域的组，并且将这些组嵌套在具有通用作用域的组内。使用该策略，对具有全局作用域的组中的任何成员身份的更改都不影响具有通用作用域的组。

具有通用作用域的组成员身份不应频繁更改，因为对这些组成员身份的任何更改都将引起整个组的成员身份复制到树林中的每个全局编录中。有关通用组和复制的详细信息，请参阅全局编录和复制。

(4) 更改组作用域

在默认情况下，新建组将被配置为具有全局作用域的安全组，而与当前域的功能级别无关。在 Windows Server 2008 系统的域中，允许对组作用域进行如下转换：

- 全局到通用。只有当要更改的组不是另一个全局作用域组的成员时，允许进行该转换。
- 本地域到通用。只有当要更改的组没有另一个本地域组作为其成员时，允许进行该转换。
- 通用到全局。只有当要更改的组没有另一个通用组作为其成员时，允许进行该转换。
- 通用到本地域。该操作没有限制。

(5) 不同作用域功能对比

Windows Server 2008 系统支持的 3 种组作用域类型的功能区别如表 5-1 所示。

表 5-1　不同组作用域之间的区别

本 地 域	全　局	通　用
当域功能级别被设置为 Windows 2000 本机或 Windows Server 2003 时，本地域组的成员可包括来自任何域的账户、全局组或通用组，以及来自相同域的本地域组	当域功能级别被设置为 Windows 2000 本机或 Windows Server 2003 时，全局组的成员可包括来自相同域的账户或全局组	当域功能级别被设置为 Windows 2000 本机或 Windows Server 2003 时，通用组的成员可包括来自任何域的账户、全局组和通用组
当域功能级别被设置为 Windows 2000 本机或 Windows Server 2003 时，本地域组的成员可包括来自任何域的账户或全局组	当域功能级别被设置为 Windows 2000 混合时，全局组的成员可包括来自相同域的账户	当域功能级别被设置为 Windows 2000 混合时，不能创建具有通用组的安全组
组可被添加到其他本地域组并且仅在相同域中指派权限	组可被添加到其他组并且在任何域中指派权限	当域功能级别被设置为 Windows 2000 本机或 Windows Server 2003 时，组可被添加到其他组并在任何域中指派权限
只要组不把具有本地域作用域的其他组作为其成员，就可转换为通用作用域	只要组不是具有全局作用域的任何其他组的成员，就可以转换为通用作用域	组可转换为本地域作用域。只要组中没有其他通用组作为其成员，就可以转换为全局作用域

2. 组类型

在 Active Directory 中有两种类型的组：通讯组和安全组。使用通讯组可以创建电子邮件通讯组列表，使用安全组则可给共享资源指派权限。组有以下特点：

- 对组设置的权限将自动应用在组中的所有对象上，可以大大简化管理员的工作。
- 组可以位于 Active Directory 中，也可以位于本地的独立计算机中。
- 组属性由作用域和类型决定。
- 可以嵌套，即可以将一个组添加到另一个组中。

(1) 通讯组

在电子邮件应用程序中，管理员可以使用“通讯组”将电子邮件同时发送给一组用户。通讯组不使用 Windows Server 的安全机制，但是可以在“对象访问控制列表(ACL)”中出现。如果需要使用组来控制对共享资源的访问，则需要使用安全组。

(2) 安全组

安全组提供了一种有效的方式来指派对网络上资源的访问权。与通讯组不同，安全组可以使用 Windows Server 的安全机制，并且可以根据需要添加到随机访问控制列表(ACL) 中。使用安全组，可以带来以下功能方面的安全性。

- 将用户权利指派到 Active Directory 中的安全组
  管理员可以对安全组指派用户权利，以确定该组的哪些成员可在域(或林)作用域内工作。在安装 Active Directory 时，系统会自动将用户权利指派给某些安全组，以帮助管理员定义域中人员的管理角色。例如，在 Active Directory 中，被添加到 Backup Operators 组的用户能够备份和还原域中每个域控制器上的文件和文件夹。因为在默认情况下，系统已经将备份和还原目录的用户权利自动指派给 Backup Operators 组，组中的用户继承该组的用户权利设置。
  可以使用组策略将用户权利指派给安全组，以帮助委派特定任务。在指派委派的任务时始终应谨慎操作，应避免为非必要用户指派过高的权利，以免产生安全隐患。
- 给安全组指派对资源的权限
  用户权利和权限不应混淆。对共享资源的权限将指派给安全组。权限决定了哪些用户可以访问该资源以及访问的级别，例如，是读取还是完全控制。系统将自动指派域对象的某些权限，以允许对默认安全组(例如 Account Operators 组或 Domain Admins 组)进行多级别的访问。
  在定义对资源和对象的权限的 ACL 中列出了安全组。为资源指派权限时，管理员应将那些权限指派给安全组而非单个用户。权限可以直接指派到组，而不是逐个指派给组中单独的用户。添加到组的每个账户，都将接受在 Active Directory 中指派给该组的权利，以及在资源上为该组定义的权限。

(3) 安全组和通讯组之间的转换

域功能级别设置为 Windows 2000 本机、Windows Server 2003 或 Windows Server 2008 模式时，管理员可以将安全组转换为通讯组，反之亦然。当域功能级别被设置为 Windows 2000 混合模式时，不可以转换组。

3. 更改组作用域或类型

组作用域直接决定组中账户的应用范围，而组类型则决定用户账户可以行使的功能。应用过程中，管理员可以根据需要，更改域用户组的作用域和类型。需要注意的是，如果域功能级别为 Windows 2000 混合模式，则无法完成此过程。Windows Server 2008 系统的默认域功能级别为 Windows 2000 纯模式，并且已经删除了混合模式，所以可以直接更改。

打开“Active Directory 用户和计算机”控制台，双击欲更改的用户组(以 coolpen 组为例)，显示如

图 5-47 所示的“coolpen 属性”对话框，在“常规”选项卡的“组作用域”和“组类型”选项区域，重新选择指定的选项即可。

图 5-47　“coolpen 属性”对话框

5.2.5　删除组

在“Active Directory 用户和计算机”窗口中，右击要删除的组并选择快捷菜单中的“删除”命令，即可删除该组。需要注意的是，随着用户组的删除，通过该组所赋予成员账户的权限也会被删除，但组内的成员不会被删除。

5.2.6　默认组介绍

安装 Windows Server 2008 和 Active Directory 域时已经自动创建了一些用户组，可以帮助管理员控制网络用户对共享资源的访问，并委派特定的域范围的管理角色。当将用户添加到组中时，用户将接受指派给该组的所有用户权利，以及指派给该组的有关任何共享资源的所有权限。

1. 默认本地组权利概述

Windows Server 2008 安装完成后，自动创建默认的本地用户组及描述如表 5-2 所示。

表 5-2　内置本地组及描述

账　户	描　述
Administrators	该组的成员具有对服务器的完全控制权限，并且可以根据需要向用户指派用户权利和权限。管理员账户也是默认成员。当该服务器加入域中时，组会自动添加到该组中。由于该组可以完全控制服务器，所以向该组添加用户时请谨慎
Backup Operators	该组的成员可以备份和还原服务器上的文件，而不管保护这些文件的权限如何。这是因为执行备份任务的权利要高于所有文件权限。他们不能更改安全设置
Certificate Service DCOM Access	允许该组的成员连接到企业中的证书颁发机构
Cryptographic Operators	授权成员执行加密操作
Distributed COM Users	成员允许启动、激活和使用此计算机上的分布式 COM 对象
Event Log Readers	此组的成员可以从本地计算机中读取事件日志
Guests	该组的成员拥有一个在登录时创建的临时配置文件，在注销时，该配置文件将被删除。来宾账户(默认情况下已禁用)也是该组的默认成员
HelpServicesGroup	该组允许管理员将对所有支持应用程序的权利设置成公用的。默认情况下，该组的唯一成员是与 Microsoft 支持应用程序相关的账户，例如远程协助。不要在该组中添加用户
Network Configuration Operators	该组的成员可以更改 TCP/IP 设置并更新和发布 TCP/IP 地址。该组中没有默认的成员
Performance Monitor Users	该组的成员可以从本地服务器和远程客户端监视性能计数器，而不用成为 Administrators 或 Performance Log Users 组的成员

续表

账　户	描　述
Performance Log Users	该组的成员可以从本地服务器和远程客户端，管理性能计数器、日志和警报，而不用成为 Administrators 组的成员
Power Users	该组的成员可以创建用户账户，然后修改并删除所创建的账户。他们可以创建本地组，然后在他们已创建的本地组中添加或删除用户。还可以在 Power Users 组、Users 组和 Guests 组中添加或删除用户。成员可以创建共享资源并管理所创建的共享资源。他们不能取得文件的所有权、备份或还原目录、加载或卸载设备驱动程序，或者管理安全性以及日志
Print Operators	该组的成员可以管理打印机
Remote Desktop Users	该组的成员可以远程登录服务器
Replicator	Replicator 组支持复制功能。Replicator 组的唯一成员应该是域用户账户，用于登录域控制器的“复制程序”服务。不能将实际用户的用户账户添加到该组中
Users	该组的成员可以执行一些常见任务，例如运行应用程序、使用本地和网络打印机以及锁定服务器。用户不能共享目录或创建本地打印机。默认情况下，Domain Users、Authenticated Users 以及 Interactive 组是该组的成员。因此，在域中创建的任何用户账户都将成为该组的成员
TelnetClients	该组的成员可以访问此系统上的 Telnet 服务器

2. 默认域用户组权利概述

默认域用户组位于活动目录的“Builtin”容器和“Users”容器中。管理员可以根据需要，将这些容器中的组移动到域中的其他组或组织单位，但不能将组移动到其他域。

(1) Builtin 容器中的组

Builtin 容器包含使用本地域作用域定义的默认组。如表 5-3 所示为 Builtin 容器中的默认组及相关描述。

表 5-3　Builtin 容器中的默认组

组	描　述
Account Operators	该组的成员可以创建、修改和删除位于 Users 或 Computers 容器中的用户、组和计算机的账户以及该域中的组织单位，但 Domain Controllers 组织单位除外。该组的成员无权修改 Administrators 或 Domain Admins 组，也无权修改这些组的成员的账户
Administrators	该组的成员具有对域中所有域控制器的完全控制。默认情况下，Domain Admins 和 Enterprise Admins 组是 Administrators 组的成员。Administrator 账户也是默认成员。由于该组在此域中具有完全控制权限，因此在添加用户时要特别谨慎
Backup Operators	该组的成员可备份和还原该域中域控制器上的所有文件，而不用考虑其各自对这些文件的权限。Backup Operators 还可以登录到域控制器并将其关闭。该组没有默认的成员。由于该组对域控制器有重要作用，因此在添加用户时要特别谨慎
Guests	默认情况下，Domain Guests 组是该组的成员。Guest 账户(默认情况下禁用此账户)也是该组的默认成员

续表

组	描　述
Incoming Forest Trust Builders(仅出现在林根域中)	该组的成员可创建对林根域的单向传入林信任。例如，驻留在 A 林中的该组成员能够创建来自 B 林的单向传入林信任。该单向传入林信任允许 A 林中的用户访问位于 B 林中的资源。该组的成员在林根域上会得到“创建传入林信任”权限。该组没有默认的成员
Network Configuration Operators	该组的成员可更改 TCP/IP 设置并续订和发布该域中域控制器上的 TCP/IP 地址。该组没有默认的成员
Performance Monitor Users	该组的成员可在本地或从远程客户端监视该域中域控制器上的性能计数器，不必成为 Administrators 或 Performance Log Users 组的成员
Performance Log Users	该组的成员可在本地或从远程客户端管理该域中域控制器上的性能计数器、日志和警报，不必成为 Administrators 组的成员
Pre-Windows 2000 Compatible Access	该组的成员具有对该域中所有用户和组的读取访问权限。该组向后兼容运行 Windows NT 4.0 及更低版本的计算机。默认情况下，特殊的 Everyone 标识是该组的成员。仅当用户在运行 Windows NT 4.0 或更低版本时，将其添加到该组中
Print Operators	该组的成员可管理、创建、共享和删除连接到该域中域控制器上的打印机。他们可以管理该域中的 Active Directory 打印机对象。该组的成员可本地登录到该域的域控制器中，并可将其关闭。该组没有默认的成员。由于该组的成员可在该域的所有域控制器上加载和卸载设备驱动程序，因此在添加用户时要特别谨慎
Remote Desktop Users	该组的成员可远程登录到该域的域控制器。该组没有默认的成员
Replicator	该组支持目录复制功能，并由该域的域控制器上的“文件复制”服务使用。该组没有默认的成员。不向该组添加用户
Server Operators	在域控制器上，该组的成员可进行交互式登录、创建和删除共享资源、启动和停止某些服务、备份和还原文件、格式化硬盘，以及关闭计算机。该组没有默认的成员。由于该组对域控制器有重要作用，因此在添加用户时要特别谨慎
Users	该组的成员可执行大部分常见任务，如运行应用程序、使用本地和网络打印机，以及锁定服务器。默认情况下，Domain Users 组、Authenticated Users 或 Interactive 都是该组的成员。因此，域中创建的任意用户账户均为该组成员



提示：由于该容器中的所有用户组都是系统默认创建的，因此，对于控制器有着非常重要的作用，操作时应倍加谨慎。

(2) Users 容器中的组

Users 容器则包含通过全局作用域定义的组和通过本地域作用域定义的组。如表 5-4 所示为 Users 容器中默认组及相关描述。

表 5-4　Users 容器中的组

组	描　述
Allowed RODC Password Replication Group	允许将此组中成员的密码复制到域中的所有只读域控制器。该组没有默认的成员

续表

组	描　述
Cert Publishers	该组的成员获准为用户和计算机发行证书。该组没有默认的成员
Denied RODC Password Replication Group	不允许将此组中成员的密码复制到域中的所有只读域控制器
DnsAdmins(随 DNS 安装)	该组的成员具有对 DNS Server 服务的管理访问权限。该组没有默认的成员
DnsUpdateProxy(随 DNS 安装)	该组的成员是可代表其他客户端(如 DHCP 服务器)执行动态更新的 DNS 客户端。该组没有默认的成员
Domain Admins	该组的成员具有对该域的完全控制权。默认情况下，该组是加入到该域中的所有域控制器、所有域工作站和所有域成员服务器上的 Administrators 组的成员。默认情况下，Administrator 账户是该组的成员。由于该组在此域中具有完全控制权限，因此在添加用户时要特别谨慎
Domain Computers	该组包含加入到此域的所有工作站和服务器。默认情况下，创建的任何计算机账户都会自动成为该组的成员
Domain Controllers	该组包含此域中的所有域控制器
Domain Guests	该组包含所有域来宾
Domain Users	该组包含所有域用户。默认情况下，此域中创建的任何用户账户都会自动成为该组的成员。可以使用该组来表示此域中的所有用户。例如，如果想要所有域用户具有对打印机的访问权限，可将打印机的访问权限指派给该组(或者将 Domain Users 组添加到打印机服务器上某个具有打印机访问权限的本地组中)
Enterprise Admins(仅出现在林根域中)	该组的成员具有对林中所有域的完全控制权限。默认情况下，该组是林中所有域控制器上 Administrators 组的成员。默认情况下，Administrator 账户是该组的成员。由于该组在林中具有完全控制权限，因此在添加用户时要特别谨慎
Enterprise Read-only Domain Controllers	无
Group Policy Creator Owners	该组的成员可修改此域中的组策略。默认情况下，Administrator 账户是该组的成员。由于该组在此域中有重要的作用，因此在添加用户时要特别谨慎
IIS_WPG(随 IIS 安装)	IIS_WPG 组是 Internet 信息服务(IIS)6.0 工作进程组。在 IIS6.0 的工作范围内存在服务于特定命名空间的工作进程。例如，www.microsoft.com 是由一个工作进程提供的命名空间，可在添加到 IIS_WPG 组的某个标识(如 Microsoft Account)下运行。该组没有默认的成员
RAS and IAS Servers	该组中的服务器获准访问用户的远程访问属性
Schema Admins(仅出现在林根域中)	该组的成员可修改 Active Directory 架构。默认情况下，Administrator 账户是该组的成员。由于该组在林中有重要的作用，因此在添加用户时要特别谨慎

5.3　用户权限的安全

使用用户账户可以登录到域或其他计算机中，从而获得对计算机网络资源的访问权。经常访问网络的用户都应当拥有网络唯一的用户账户，并且根据用户的职责不同，分配不同的用户权限，同时，设置严格

的用户策略，保护用户账户的安全。

5.3.1　为用户设置权利

用户权利可以从组策略中指派，也可以从独立服务器上的“本地安全策略”和域控制器上的“默认域控制器安全策略”中指派，并且被设置的对象可以是单个用户，也可以是用户组。例如，要限制用户的登录失败的次数，使试图登录计算机的非法用户在尝试 5 次后，自动将账户锁定，以确保账户安全。

① 依次选择“开始”→“管理工具”→“本地安全策略”选项，打开“本地安全策略”窗口。依次展开“安全设置”→“账户策略”→“账户锁定策略”选项，如图 5-48 所示。

② 双击“账户锁定阈值”策略，显示如图 5-49 所示的“账户锁定阈值 属性”对话框。“×次无效登录”微调框的默认值为 0，即不限制登录次数，永远不会锁定账户，在其中输入“5”即可。

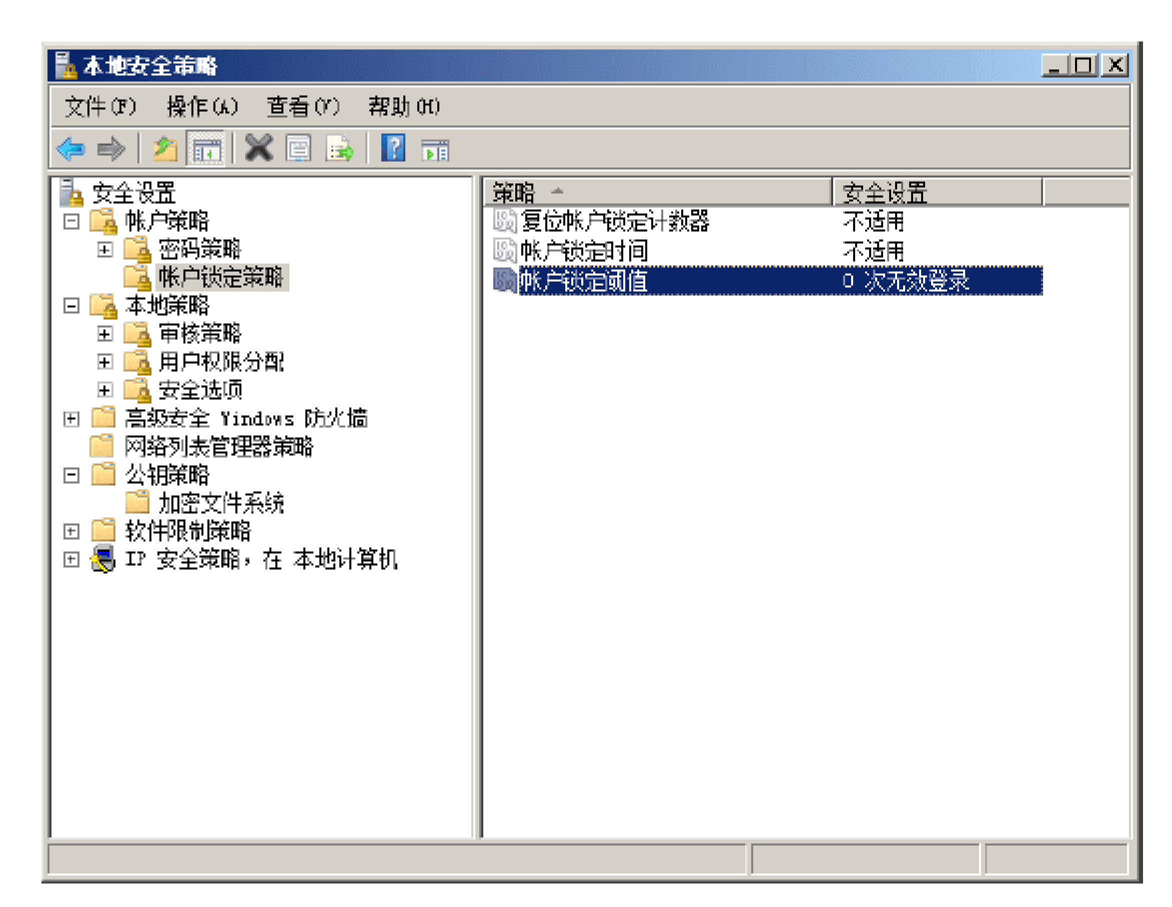




图 5-48　“本地安全策略”窗口

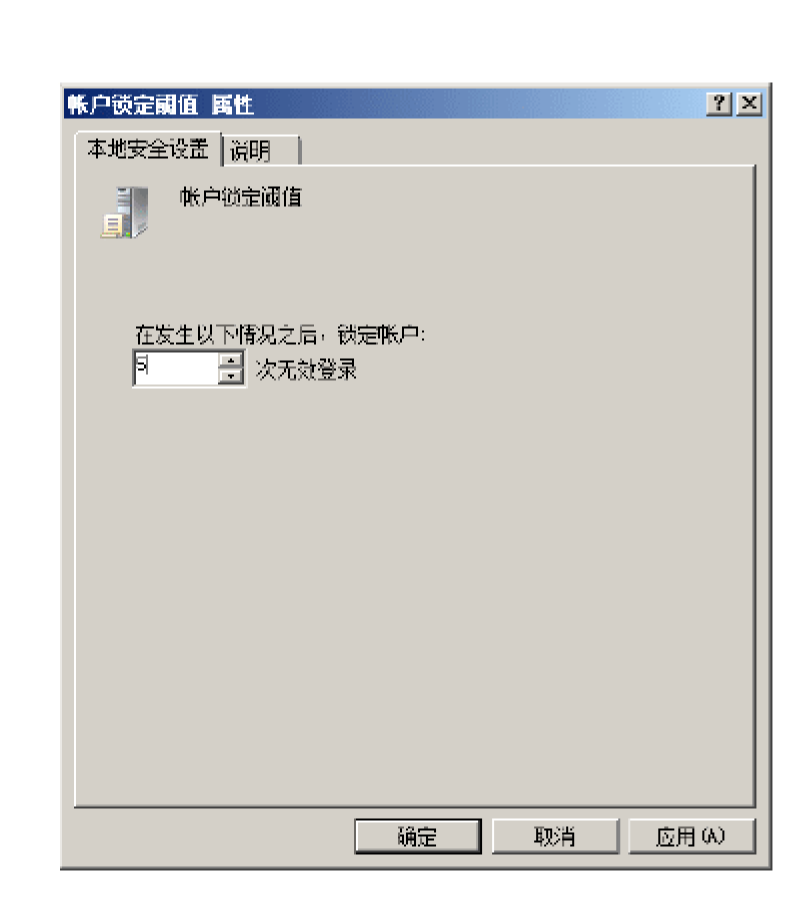


图 5-49　“账户锁定阈值 属性”对话框

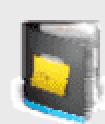
③ 单击“确定”按钮，保存设置。

这样，当用户再次登录时，如果连续 5 次输入密码不正确，就会被锁定，并显示如图 5-50 所示的“登录消息”提示框，提示账户不能登录。



图 5-50　“登录消息”提示框

如果计算机中的用户账户比较多，建议将用户添加到组，并允许组内的用户继承组的权利设置。但是，对于一些比较重要的组，应取消权限继承设置，然后再根据不同用户的身份，以决定是否允许继承组的权限。



提示：如果是在域控制器上配置该权限，在需要在“组策略管理编辑器”窗口中，修改 Default Domain Controllers Policy 策略中的相关设置。

5.3.2　将用户权利指派到组

为避免权限管理混乱，应尽量将用户权利指派到组，然后将需要获得此权限的用户添加到该组中，尤其是对于用户较多的域网络，更应如此。如果是 Windows Server 2008 域网络，则可以在域控制器的“组策略管理”工具中，编辑域控制器的默认策略 Default Domain Controllers Policy 或者“本地安全策略”中

的相关设置。如果是独立服务器，则只能在“本地安全策略”中完成。

① 在 Windows Server 2008 域控制器上，依次选择“开始”→“管理工具”→“本地安全策略”选项，打开“本地安全策略”窗口。

② 依次展开“安全设置”→“本地策略”→“用户权限分配”选项，在右侧窗口中列出了可以分配给用户的所有用户权限，如图 5-51 所示。

③ 双击要分配给组的权限，打开属性对话框，添加要指派给的组名即可。例如，双击“从网络访问此计算机”策略，显示如图 5-52 所示的“从网络访问此计算机 属性”对话框。从列表中显示具备此权利的用户或者组。

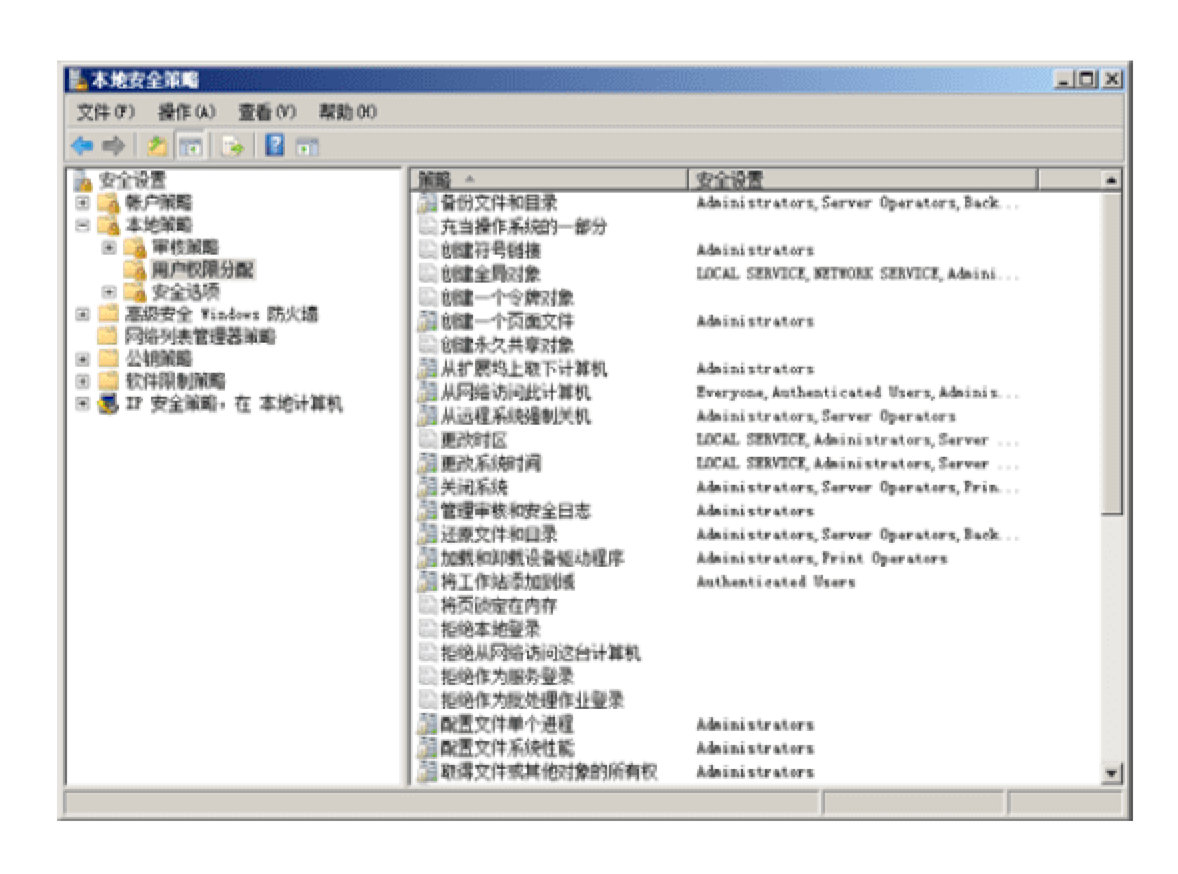


图 5-51 “本地安全策略”窗口

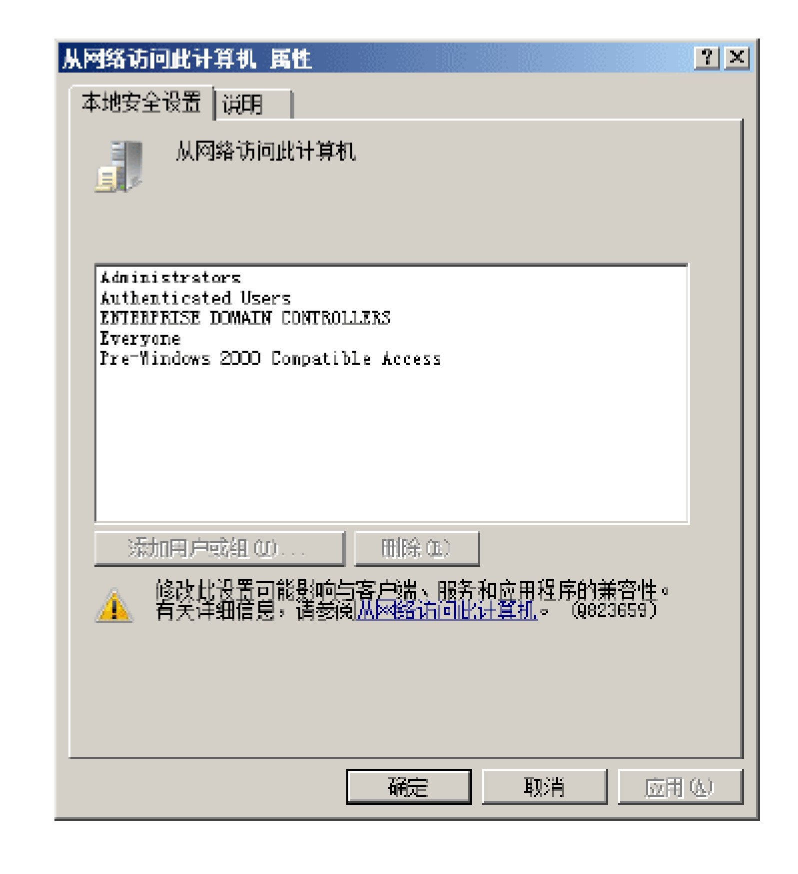


图 5-52 “从网络访问此计算机 属性”对话框

当为组分配了某个权限以后，该组中的用户同时也会拥有该权限，而以后向该组中添加用户时，新用户也会拥有此权限。

通常情况下，可参考如下说明将适当的权限分配给相应的用户组：

- 管理员组(Administrators)可以被授权的权利包括更改系统事件、创建页面文件、装载和卸载设备驱动程序、在本地登录、管理审核安全日志、配置单一进程、配置系统性能、关闭系统、取得文件或者对象的所有权。
- 备份操作员组(Backup Operators)可以被授权的权利包括备份文件和目录、在本地登录、还原文件和目录(如果不想让备份操作员组具备还原文件和目录的权利，可以重建一个新的用户组)。
- 用户组可以被授权的权利为在本地登录(默认的)。
- 将有关“Everyone”组的权利删除。尤其是在 Windows 2000 系统中，默认情况下，Everyone 组被赋予“完全控制”权限，毫无疑问，对系统安全而言，这是非常危险的。
- 将有关“Power Users”组的权利删除。

不授予任何权利，除非应用程序有特殊的要求，必须取消其他所有默认状况下的权利设定。

5.4 用户环境安全

用户工作环境主要是指用户桌面、登录设置、网络连接等，这些基本设置可以保证用户快速投入自己的工作。并且默认情况下，许多常用的用户信息都被保存在以用户名命名的目录下，如文档、图片、视频

等，这些信息不仅容易被恶意用户窃取，而且如果系统发生故障，也容易导致数据丢失。通过对常用且重要的用户进行重定向，即可避免此类情况的出现。

5.4.1 重定向用户配置文件

在 Windows Server 2008 系统中，所有用户账户的配置文件都被保存在系统分区的“用户”文件夹中，并且为每个账户单独保存，包括收藏夹、桌面、文档、视频、联系人等重要信息。当系统崩溃或重新安装操作系统时，一旦忘记备份，这些数据将全部丢失。所以最好的方法就是，将这些重要内容重定向到其他非系统分区的安全目录下。

① 在资源管理器中，打开系统分区的“用户”→“tianjl(用户账户名)”文件夹，显示如图 5-53 所示的窗口，这是当前用户账户的所有配置文件。

② 以“桌面”文件夹为例，右击并选择快捷菜单中的“属性”命令，打开“桌面 属性”对话框，切换到如图 5-54 所示的“位置”选项卡。

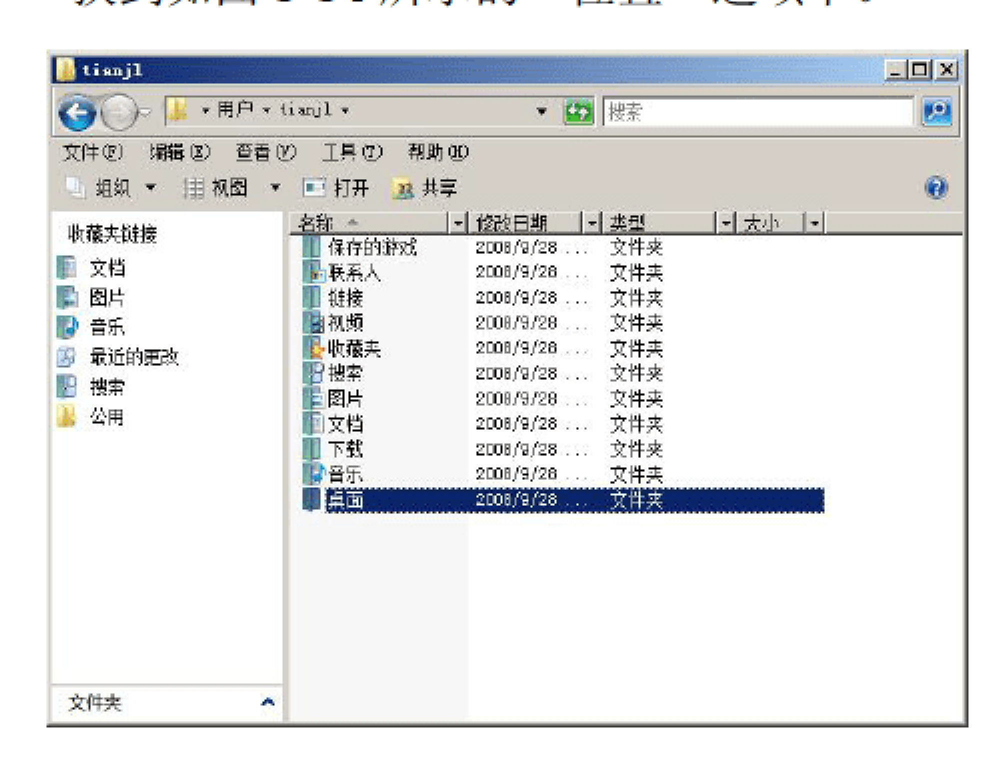


图 5-53 用户的所有配置文件

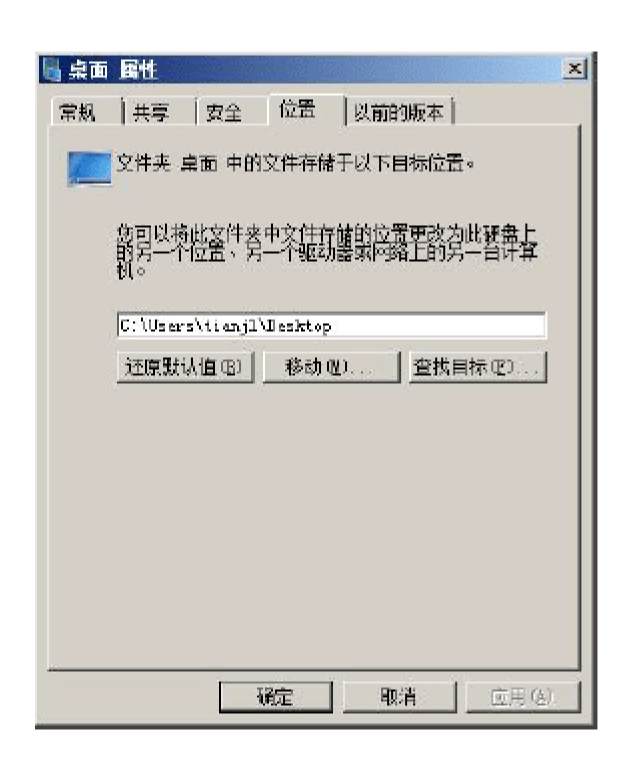


图 5-54 “位置”选项卡

③ 单击“移动”按钮，打开如图 5-55 所示的“选择一个目标”对话框。选择其他分区上的某个特定文件夹即可。

④ 单击“选择文件夹”按钮，返回“桌面 属性”对话框，单击“确定”按钮，显示如图 5-56 所示的“移动文件夹”对话框，提示是否确认移动。

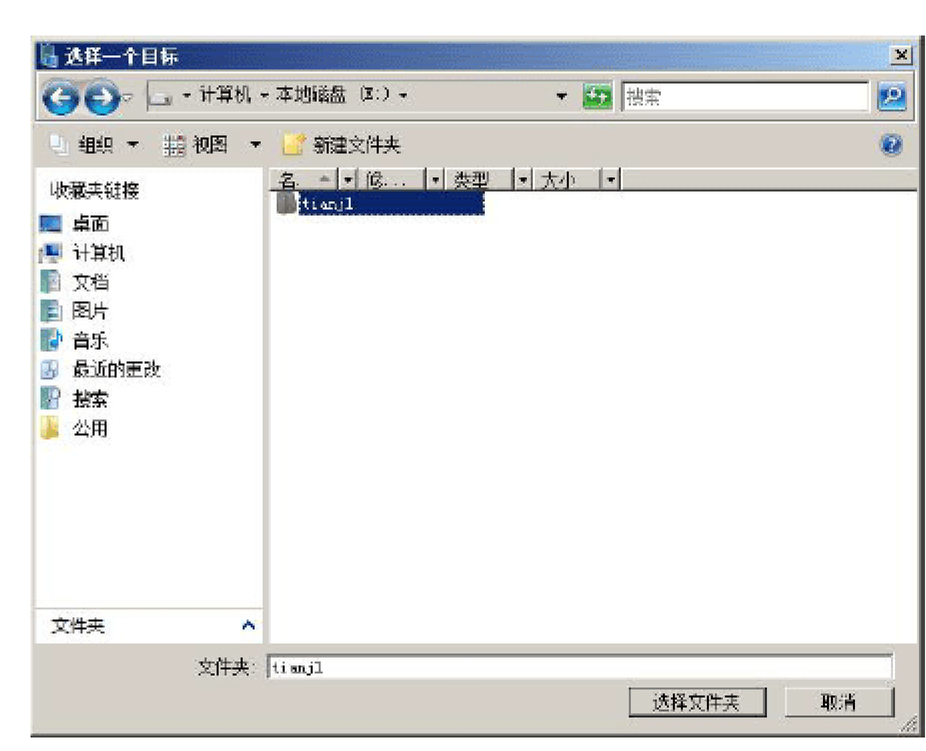


图 5-55 “选择一个目标”对话框

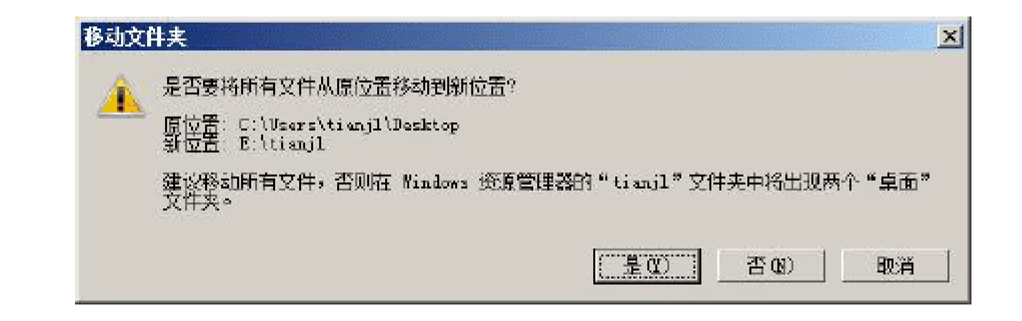
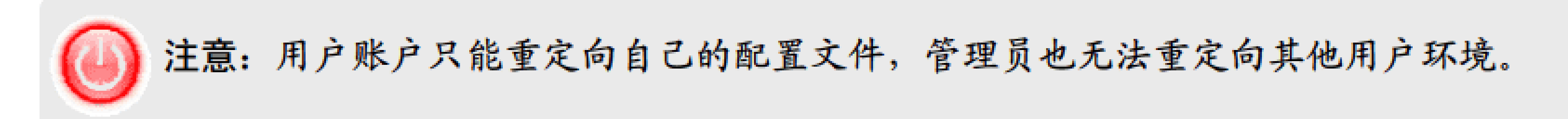


图 5-56 “移动文件夹”对话框

⑤ 单击“是”按钮，完成设置。用户配置文件中，其他目录的重定向，与此完全相同，这里不复赘述。


注意：用户账户只能重定向自己的配置文件，管理员也无法重定向其他用户环境。

5.4.2 重定向程序安装目录“Program Files”

所有用户的默认应用程序安装目录都是%Systemroot%\ Program Files，随着安装文件的增多，此文件夹会占用大量的空间，并且安装目录固定也不利于应用程序的安全。通过修改注册表即可将默认安装目录，重定向到其他分区甚至其他磁盘。

① 单击“开始”按钮，显示“开始”菜单，在“开始搜索”文本框中输入“regedit”并按 Enter 键，打开如图 5-57 所示的“注册表编辑器”窗口。依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion 分支。

② 在右侧的列表框中双击 ProgramFilesDir 键值，显示如图 5-58 所示的“编辑字符串”对话框。在“数值数据”文本框中输入“D:\Program Files”，将系统默认的“C:\Program Files”目录，重定向到 D:\Program Files 目录中。

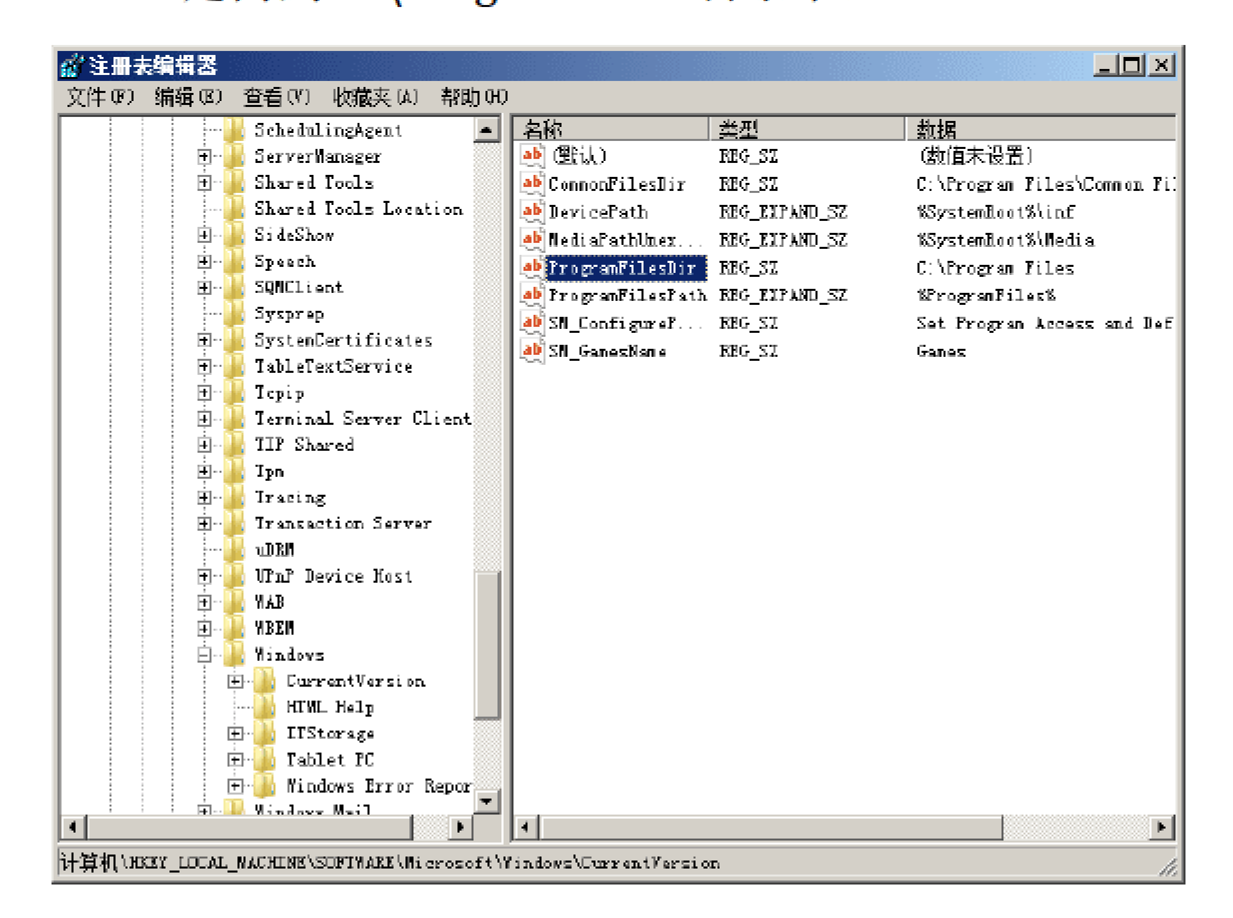


图 5-57 “注册表编辑器”窗口



图 5-58 “编辑字符串”对话框

③ 单击“确定”按钮，完成安装目录的更改。

④ 重新启动系统，设置生效。

5.4.3 重定向“IE 临时文件夹”

服务器虽不经常上网，但偶尔也会由于业务需要访问 Internet，使用 IE 浏览器浏览网页时，会产生一些临时文件，随着时间的积累，这些临时文件就会非常庞大，不仅占用宝贵的系统分区空间，而且容易留下安全隐患。通过将保存临时文件的文件夹重定向到其他分区，即可解决该问题。

① 打开 IE 浏览器，在菜单栏中选择“工具”|“Internet 选项”命令，显示如图 5-59 所示的“Internet 选项”对话框。

② 切换到“常规”选项卡，在“浏览历史记录”选项区域中，单击“设置”按钮，显示如图 5-60 所示的“Internet 临时文件和历史记录设置”对话框。

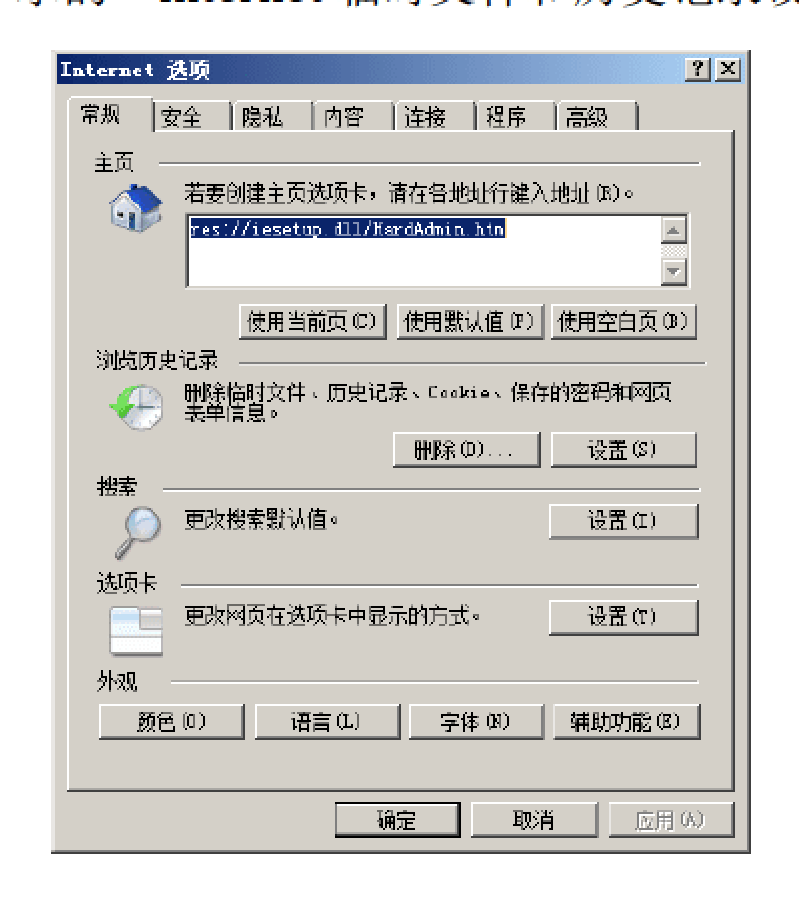


图 5-59　“Internet 选项”对话框



图 5-60　“Internet 临时文件和历史记录设置”对话框

③ 系统默认的临时文件夹的位置为“C:\Users\Administrator\AppDate\Local\Microsoft\Windows Internet Files\”，要重定向到其他位置单击“Internet 临时文件”选项区域中的“移动文件夹”按钮，显示如图 5-61 所示的“浏览文件夹”对话框，选择文件夹的目标位置。

④ 单击“确定”按钮，返回到“设置”对话框。

⑤ 单击“确定”按钮，显示如图 5-62 所示的“注销”对话框。

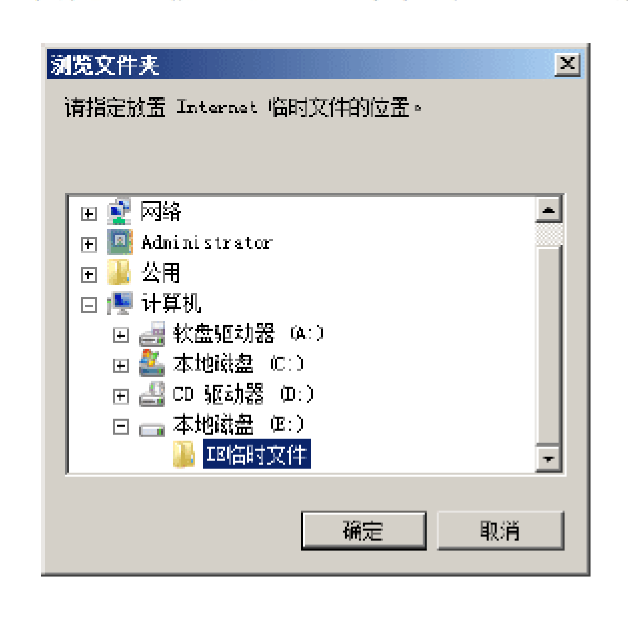


图 5-61　“浏览文件夹”对话框



图 5-62　“注销”对话框

⑥ 单击“是”按钮，系统自动执行注销操作。重新启动后，“IE 临时文件夹”生效。

5.4.4　重定向“虚拟内存”

虚拟内存是用硬盘空间来弥补计算机内存空间的缺乏，在早期比较实用，但在目前超大内存时代，也可以通过这种方法，提高系统处理速度。默认情况下，系统自动将系统分区的一部分空间作为虚拟内存，通过将虚拟内存重定向到其他分区，可以释放系统分区空间，提高系统可靠性。

① 右击“我的电脑”并选择菜单中的“属性”命令，显示如图 5-63 所示的“系统”窗口。

② 单击“高级系统设置”链接，打开“系统属性”对话框，切换到如图 5-64 所示的“高级”选项卡。

③ 在“性能”选项区域中，单击“设置”按钮，打开“性能选项”对话框，切换到如图 5-65 所示的

“高级”选项卡，显示当前系统虚拟内存大小为 1024 MB。



图 5-63 “系统”窗口

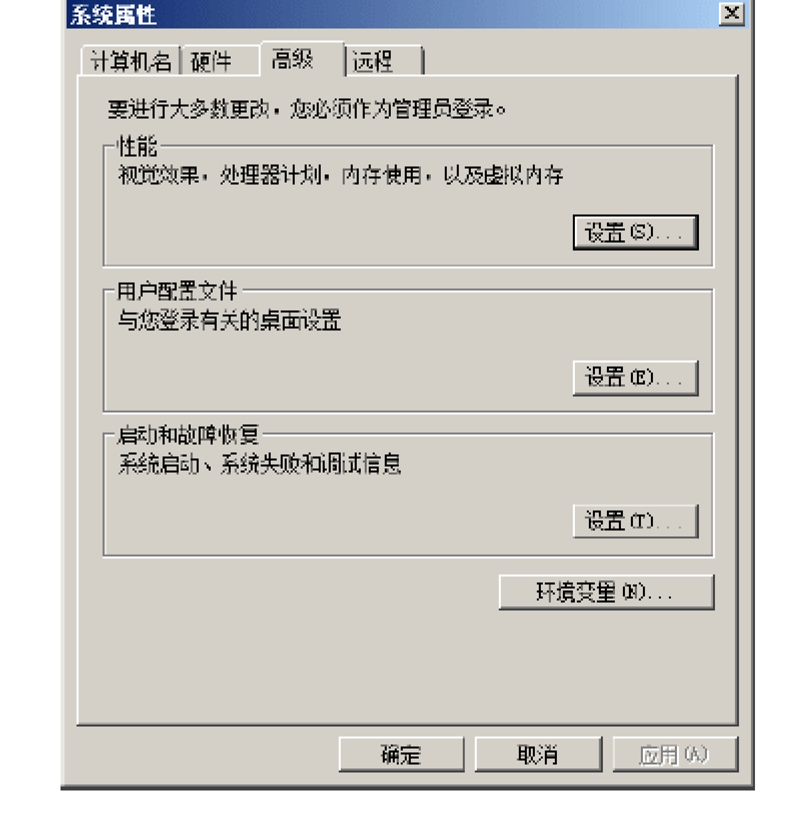


图 5-64 “高级”选项卡

④ 在“虚拟内存”选项区域中，单击“更改”按钮，显示如图 5-66 所示的“虚拟内存”对话框。取消选中“自动管理所有驱动器的分页文件大小”复选框，即可开始修改每个分区的虚拟内存设置。

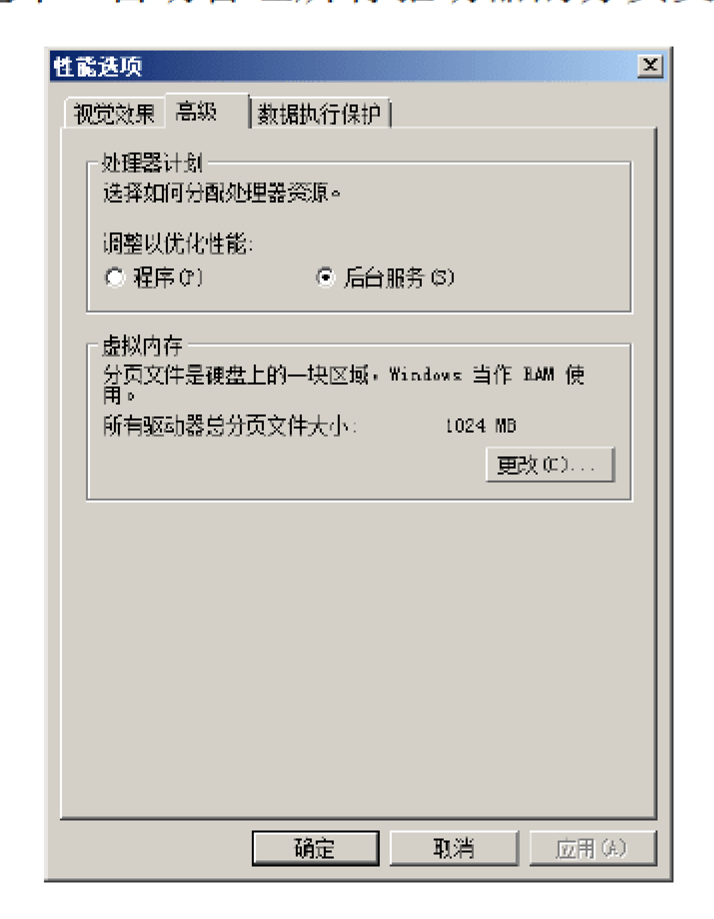


图 5-65 “性能选项”对话框

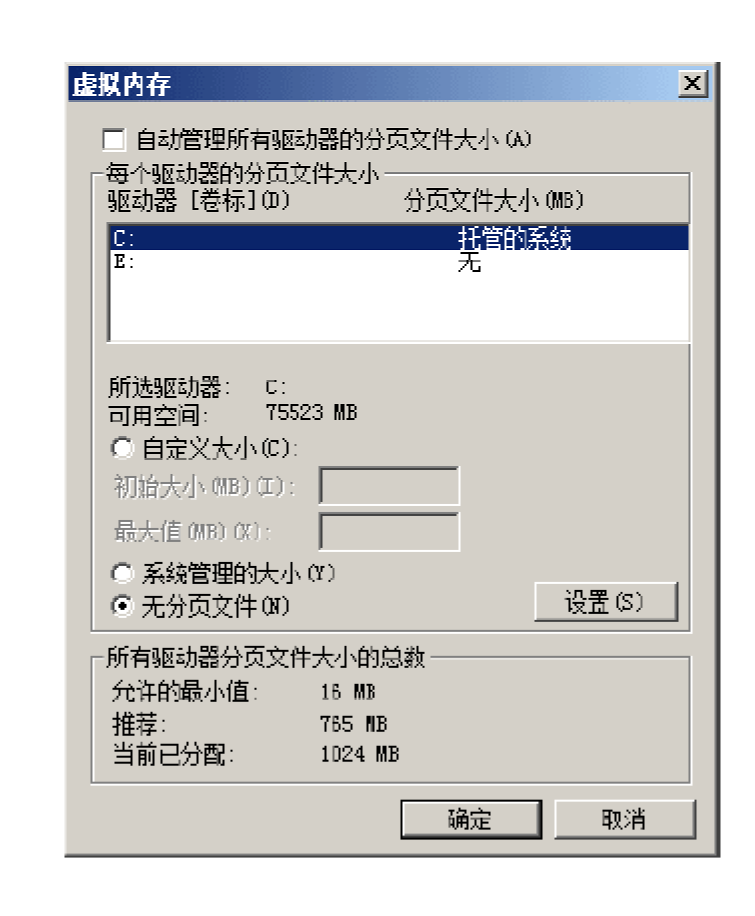


图 5-66 “虚拟内存”对话框

⑤ 在“驱动器”列表框中，选择系统默认的驱动器“C：”，在“每个驱动器的分页文件大小”选项区域中，选择“无分页文件”单选按钮，单击“设置”按钮，删除默认驱动器的性能内存设置，显示如图 5-67 所示的“系统属性”对话框。

⑥ 在“驱动器”列表框中，选择驱动器“E：”，在“每个择驱动器的分页文件大小”选项区域中，选择“自定义大小”单选按钮，在“初始大小”文本框中，输入虚拟内存的初始值，在“最大值”文本框中输入虚拟内存的最大值。单击“设置”按钮，即可完成驱动器的性能内存设置，如图 5-68 所示。虚拟内存大小通常为物理内存的 2 倍左右，可依实际情况而定。



提示：也可以选择“系统管理的大小”单选按钮，由系统自动分配适当大小的虚拟内存空间，此时“分页文件大小”也将显示为“托管的系统”状态。

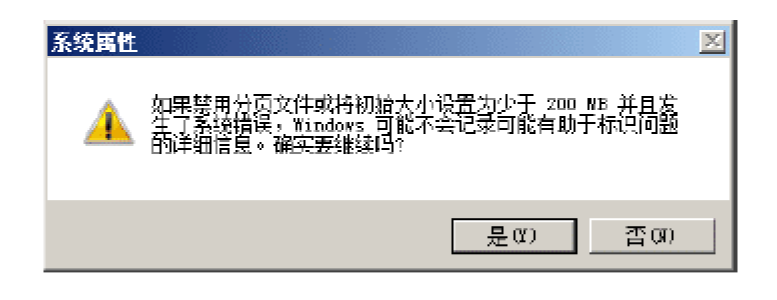


图 5-67　“系统属性”对话框

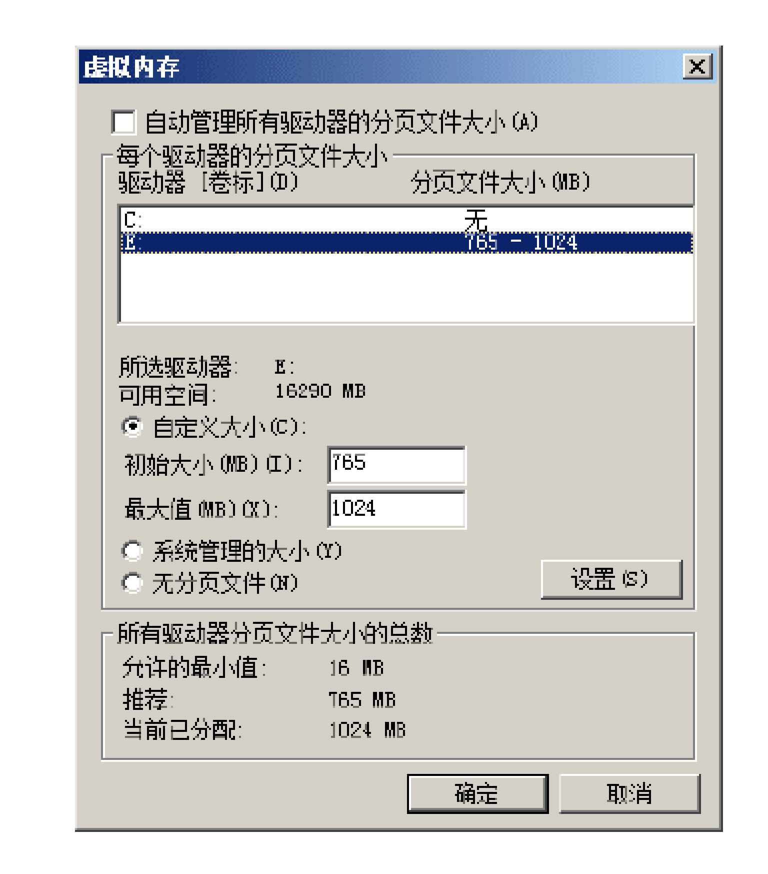


图 5-68　重定向虚拟内存

⑦ 单击 3 次“确定”按钮，关闭“系统属性”对话框。重新启动计算机，即可使设置生效。

5.5　域用户配置文件安全

用户配置文件，是用户登录时系统加载所需环境的设置和文件的集合，包括所有用户专用的配置设置，如程序项目、屏幕颜色、网络连接、打印机连接、鼠标设置及窗口的大小和位置等。当用户使用 Windows 2000 以上操作系统的计算机第一次登录到域时，就会为用户自动创建专用配置文件。

5.5.1　用户配置文件概述

用户配置文件包括所有用户专用的配置设置。用户配置文件在系统的什么位置呢？用户配置文件包括哪些内容呢？下面我们来介绍这些内容。

1. 用户配置文件类型

根据用户配置文件应用工作环境的不同，用户配置文件可分为如下 4 种配置文件类型。

- 本地用户配置文件。第一次登录到计算机时，将创建本地用户配置文件，并存储在计算机的本地硬盘上。对本地用户配置文件所做的任何更改都只是针对用户所在的计算机。
- 漫游用户配置文件。漫游用户配置文件由系统管理员创建，通常存储在服务器上。每次登录到网络上的任何一台计算机时，都可以使用该配置文件。对漫游用户配置文件所做的更改将在服务器上更新。
- 强制用户配置文件。此文件是用来为个人或整个用户组指定特殊设置的漫游配置文件。只有系统管理员才能更改强制用户配置文件。
- 临时用户配置文件。无法加载用户配置文件时所发布的临时配置文件。每次会话结束时会删除临时配置文件，当用户注销时，将丢失用户对其桌面设置和文件所做的更改。

2. 用户配置文件存储位置

成员计算机使用域用户账户登录到域后，就会在本地计算机上自动存储用户配置文件，存储位置为系

统盘(默认为 C 盘)下的 Documents and Settings 文件夹，如果是 Windows Server 2008 系统，则存储在系统盘下的“用户”文件夹中。

如果本机用户和域同名用户都在本机登录过，将在同名文件夹后面附加后缀。例如，在域(coolpen.net)中的计算机上，本地已经存在 Administrator 的账户，域上也有一个 Administrator 账户，即使用两个名称的账户以不同的方式登录过这台计算机，如果本地账户的用户配置文件夹为 Administrator，那么域用户的用户配置文件夹为 Administrator.COOLPEN，如图 5-69 所示。

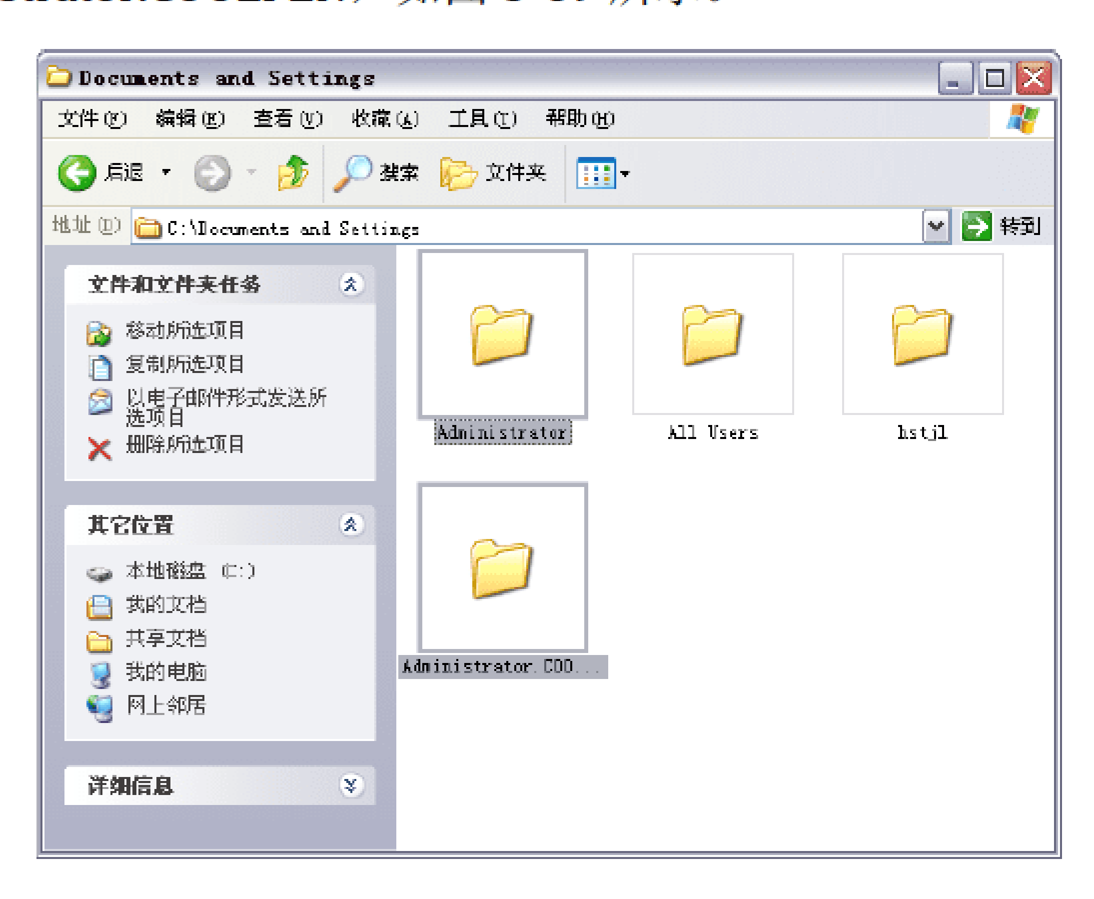


图 5-69 Documents and Settings 窗口

3. 用户配置文件夹的其他文件

Windows 为每个登录到计算机上的用户创建配置文件。除这些配置文件外，还有一些“特殊”的配置文件：

(1) 默认用户(Default User)

默认用户配置文件被用作任何新用户的起始点。当用户第一次登录到计算机时，Windows 将创建一个新文件夹，用来储存新用户的配置文件，并且将默认的配置文件复制到这个新文件夹中。用户对默认配置文件所作的更改都被记录到用户配置文件中。默认情况下，默认用户配置文件的属性是隐藏。

(2) 所有用户(All Users)

每个用户的“开始”菜单和桌面包含所有项目，这些内容来自“所有用户”的配置文件以及他或她自己的配置文件。从“所有用户”的配置文件中取得的项目被作为公用程序项，系统上的每个用户都能看到这些。如果想要保证每个登录的用户都能访问一个程序或文件，那么就将它的快捷方式放进“所有用户”的配置文件中即可，但是一定要小心，如果一个用户删除了此快捷方式或文件，对所有用户来说，都会被删除。

5.5.2 查看用户配置文件

右击“我的电脑”，在弹出的快捷菜单中选择“属性”命令，打开“系统属性”对话框，切换到“高级”选项卡，显示“高级”对话框。单击“用户配置文件”选项区域中的“设置”按钮，显示如图 5-70 所示的“用户配置文件”对话框。从图中可以看出，用户配置文件“类型”是“本地”，说明用户配置文件保存在本地。



图 5-70　查看用户配置文件

5.5.3　漫游用户配置文件

在部署 Active Directory 的网络中，所有域用户可以在域内任意一台计算机登录。当用户在一台计算机上登录并配置之后，到其他计算机上登录时，所有的设置还原为原始设置。原因是用户配置文件保存在以前登录过的计算机中。

1. 漫游用户配置文件简介

漫游用户配置文件是使用户登录到域中的计算机后，将用户配置文件存储在由管理员指定的服务器中。当用户成功登录后，用户配置文件将复制到当前登录的本地计算机中。当本地计算机上的用户配置文件修改并注销用户后，所做的更改将复制到存储在服务器上的用户配置文件中，并在下次用户登录时应用。

从“Active Directory 用户和计算机”管理控制台中，可以为用户配置文件指派服务器位置。如果用户的域账户中输入了用户配置文件的路径，当用户注销时，该用户本地用户配置文件的副本将保存到本地和用户配置文件路径位置。用户下次登录时，用户配置文件路径位置中存储的配置文件将与本地用户配置文件文件夹中的副本进行比较，然后打开最新的配置文件副本。由于存储在指定的服务器中，该本地用户配置文件将成为漫游用户配置文件。不论用户在什么地方登录，都可以使用其设置和文档。

2. 配置漫游用户配置文件

Windows Server 2008 的“Active Directory 用户和计算机”允许配置漫游用户配置文件存储位置，当用户登录后，从服务器中将用户配置文件下载到本地并加以应用。当用户注销时，将把本地的用户配置文件同步到服务器，保证服务器和本地计算机用户配置文件同步。

3. 服务器设置

① 在服务器上创建名称为“UserShare”的共享文件夹，存储用户配置文件。在共享文件夹权限设置中，将“Everyone”用户设置为“共有者”，如图 5-71 所示。

② 在“Active Directory 用户和计算机”窗口中，右击 liuxh 用户，并选择快捷菜单中的“属性”命令，显示“liuxh 属性”对话框。切换到如图 5-72 所示的“配置文件”选项卡。在“用户配置文

件”选项区域的“配置文件路径”文本框中，输入共享文件夹地址，例如“\\lxh-2008\usershare\%username%”，“lxh-2008”是域控制器的主机名。

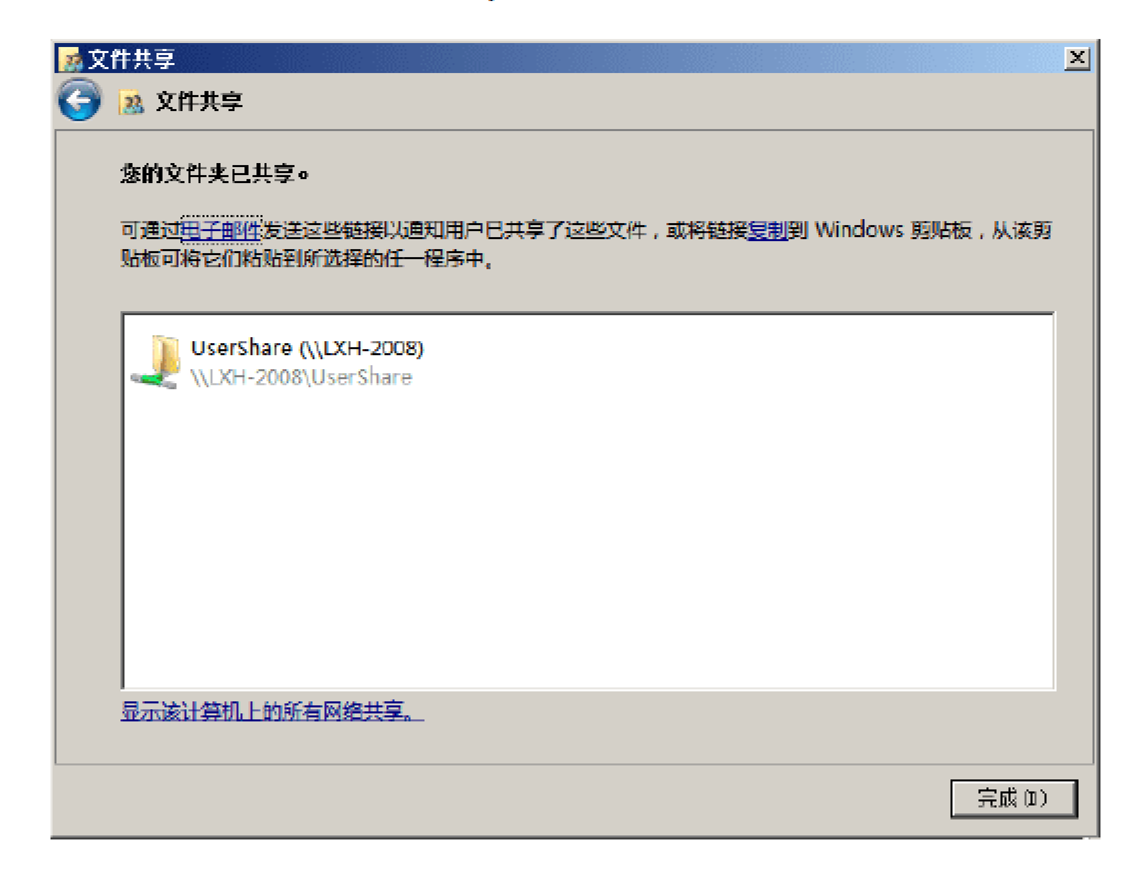


图 5-71　创建共享文件夹

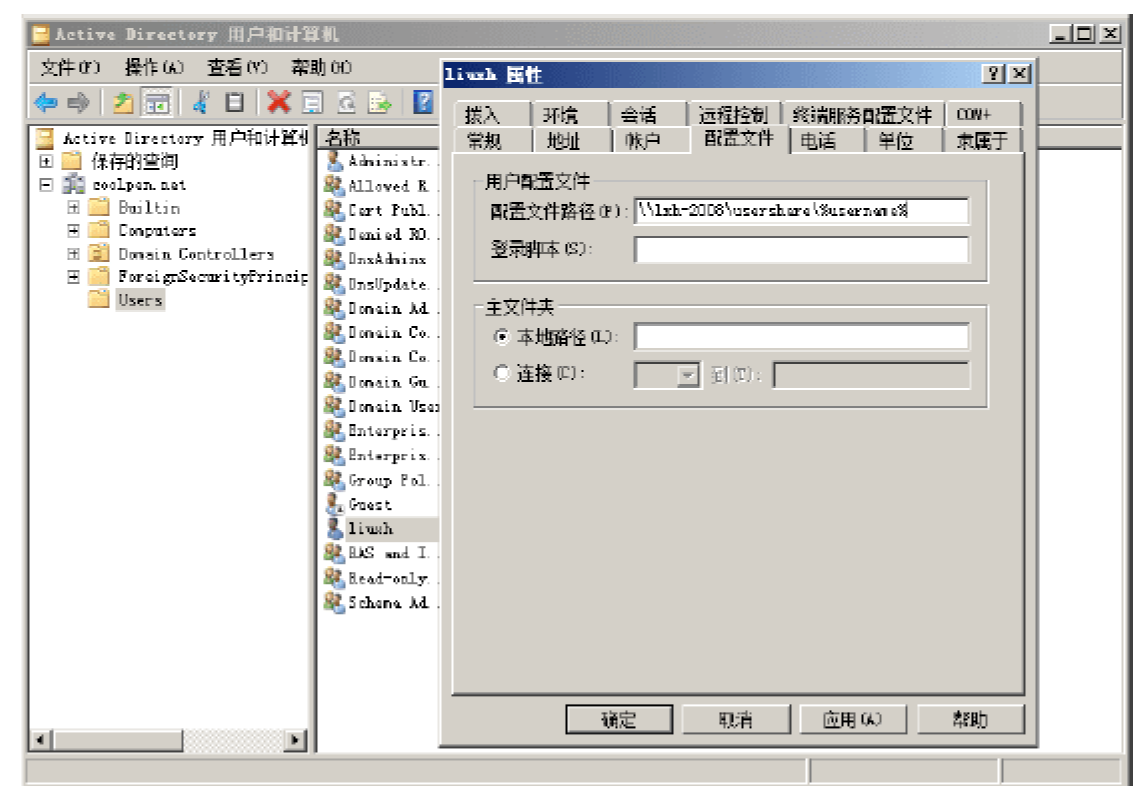


图 5-72　配置用户配置文件

③　单击“确定”按钮，设置完成域用户 liuxh 配置文件。

4. 用户配置文件验证

客户端计算机注销，重新登录到域。

①　使用“查看用户配置文件”介绍的方法，查看当前登录的用户的配置文件的类型，域用户 liuxh 配置文件类型为“漫游”，如图 5-73 所示。

②　在域控制器中，打开创建的共享文件夹 Usershare，将显示与域用户账户 liuxh 同名的文件夹 liuxh，如图 5-74 所示。域用户 liuxh 的漫游用户配置文件存储在该目录下。

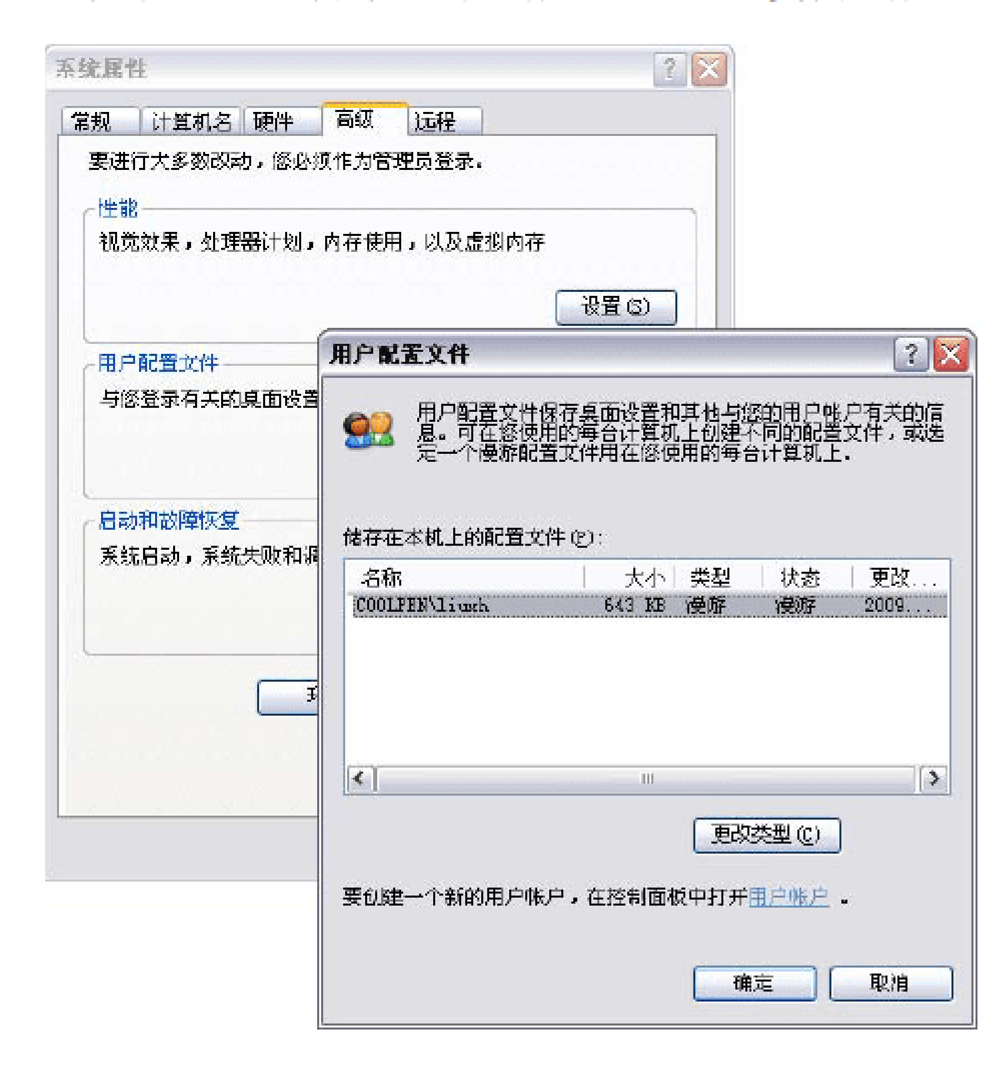


图 5-73　用户配置文件验证

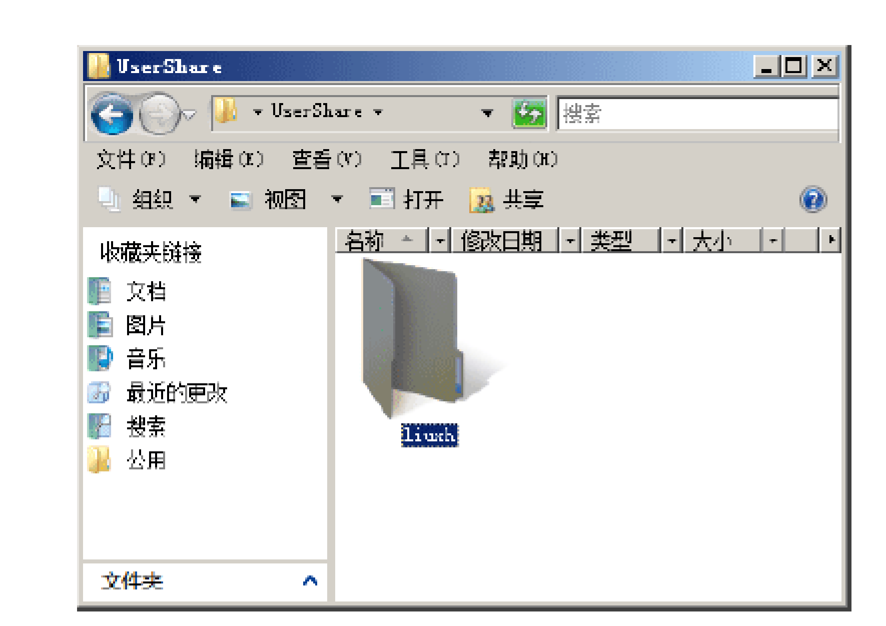


图 5-74　共享文件夹中的用户配置文件目录

③　域用户 liuxh 到其他域内计算机上登录，将显示相同的配置文件以及配置环境。

第 6 章　文件系统安全

文件安全是系统安全中最重要的课题之一，既要确保网络用户能够正常使用所需的文件，又要防止其滥用，确保文件的安全性。通常情况下，可以通过为文件设置适当的访问权限，限制用户的非法访问，达到访问控制的目的。另外，在 Windows Server 2008 系统中，还提供了 AD RMS 文件安全保护功能，可以确保局域网内文件的安全访问。

关键词

- 基于 NTFS 文件系统的安全设置
- 权限管理服务
- 共享资源安全

6.1 基于 NTFS 文件系统的安全设置

NTFS 是网络服务器上使用最多的文件系统，其主要特点是安全性高，便于网络文件安全的统一管理，允许管理员为文件配置详细的访问控制权限。Windows Server 2008 要求系统分区必须为 NTFS 文件系统，以便于为各种网络服务数据及日志信息提供更安全的存储和访问环境。

6.1.1 NTFS 权限概述

权限是指与计算机或网络上的对象(如文件和文件夹)关联的访问规则，用于确定用户是否可以访问对象，可以执行哪些操作。本地计算机管理员或域管理员可以为普通用户和组分配权限。使用 NTFS 文件系统，管理员可以实现对文件和文件夹的授权访问，从而确保服务器文件存储的安全。默认情况下，只有授予用户允许访问权限时，该用户才可以访问，否则是无法访问的。

1. NTFS 文件夹权限和 NTFS 文件权限

对于 NTFS 分区上的文件和文件夹，管理员可以通过 NTFS 权限限制不同用户账户的访问权限。文件和文件夹的 NTFS 权限有两种类型：显式权限和继承权限。其中，显式权限是系统创建对象时，默认赋予用户账户的访问和操作权限；继承权限是从父对象传播到当前对象的权限。继承权限可以减轻管理权限的任务，并且确保给定容器器内所有对象之间的权限一致性。默认情况下，文件将自动继承来自其父文件夹的 NTFS 权限设置。

(1) NTFS 文件夹权限

NTFS 文件夹权限及允许用户完成的操作如下表 6-1 所示。

表 6-1 NTFS 文件夹权限

NTFS 文件夹权限	允许用户完成的操作
读取	查看该文件夹中的文件和子文件夹； 查看文件夹的所有者、权限和属性(如只读、隐藏、存档和系统)
写入	在该文件夹内新建文件和子文件夹； 更改文件夹属性，查看文件夹的所有者和权限
列出文件夹目录	查看该文件夹中的文件和子文件夹的名称
读取及运行	完成“读取”权限和“列文件夹目录”权限所允许的操作； 漫游各个文件夹，以便访问其他文件和文件夹，即使该用户没有那些文件夹的权限
修改	完成“写入”权限及“读取及执行”权限所允许的操作； 删除文件夹
完全控制	完成其他所有 NTFS 权限允许的操作； 更改权限，取得所有权和删除子文件夹和文件

(2) NTFS 文件权限

NTFS 文件权限及允许用户完成的操作如表 6-2 所示。

表 6-2　NTFS 文件权限及允许用户完成的操作

NTFS 文件权限	允许用户完成的操作
读取	读取该文件和查看文件属性、所有者及权限
写入	覆盖该文件，更改文件属性和查看文件的所有者和权限
读取及运行	完成“读取”权限所允许的操作； 运行应用程序
修改	完成“写入”权限和“读取及运行”权限所允许的操作； 修改和删除文件
完全控制	完成其他所有 NTFS 文件权限所允许的操作； 更改权限和取得所有权

2. 访问控制列表

权限是与特定用户或组相关联的，或者是被管理员指派到用户和组的安全描述符。用户和组的每个权限的分配都会在系统中作为访问控制条目(ACE，Access Control Entries)显示，访问控制列表(ACL，Access Control Lists)就是这些访问控制条目的集合。如果 ACL 中不存在相应的 ACE，则系统将自动拒绝该用户账户访问相应资源。

访问控制列表有两种：任意访问控制列表(Discretionary ACL)和系统访问控制列表(System ACL)。任意访问控制列表包含用户和组的名称列表及其相应的权限，例如允许或拒绝等。系统访问控制列表是为审核服务的，包含对象被访问的时间。

访问控制条目包含用户或组的 SID 以及对象的权限。访问控制项有两种：允许访问和拒绝访问，其中拒绝访问的优先级高于允许访问。当使用管理工具列出对象的访问权限时，列表的排序是以文字为顺序的，并不像防火墙的规则那样由上往下的顺次执行，访问控制条目中的权限是永远不会冲突的，并且拒绝访问总是优先于允许访问的。

用户通过验证后，登录进程会分配给用户一个访问令牌，该令牌相当于用户访问系统资源的票证，即当用户试图访问系统资源时，将访问令牌提供给 Windows Server 2008 系统， 系统将收到的访问令牌与目标资源的访问控制列表核对。如果用户被允许访问该对象，Windows Server 2008 将会分配给用户适当的访问权限，否则用户将无法访问指定资源。

3. 多重 NTFS 权限

管理员可以根据需要为 NTFS 分区上的文件和文件夹同时设置 NTFS 权限，而文件夹和文件又有可能是包含与被包含的关系，所以必然会产生资源权限的重复，从而直接导致文件夹或文件最终的 NTFS 权限并非是管理员真正需要的结果。

(1) 权限是累积的

用户对一个资源的最终权限，是为该用户指定的全部 NTFS 权限和为该用户所属组指定的全部 NTFS 权限之和。如果某用户拥有一个文件夹的读取权限，同时又是对该文件夹有写入权限的用户组的成员，则最终该用户对这个文件夹既有读取权限，也有写入权限。

例如，用户账户 liuxh 隶属于 Manager 组，并且该用户本身对 Folder 文件夹具有读取权限，而其所在的用户组 Manager 对 Folder 文件夹拥有写入权限，所以最终用户 liuxh 对 Folder 文件夹的有效权限就是“读取+写入”，如图 6-1 所示。

(2) 文件权限优先于文件夹权限

NTFS 文件权限优先于 NTFS 文件夹权限，即用户只要有访问一个文件的权限，即使没有访问该文件所在文件夹的权限，也可以访问该文件。用户可以通过用通用命令规则(UNC)或本地路径，从各自的应用程序打开有权访问的文件。即使该用户由于没有包含该文件夹的权限而看不到该文件夹，但仍然可以访问那些文件。

例如，Folder 文件夹下包含 Files1 和 Files2 两个文件，Folder 的文件夹权限允许用户 liuxh 写入，但 File2 的 NTFS 权限只允许用户 liuxh 读取，则此时用户 liuxh 的有效权限就是对 Folder 文件夹(包括 File1)的写入权限和对 File2 的读取权限，如图 6-2 所示。

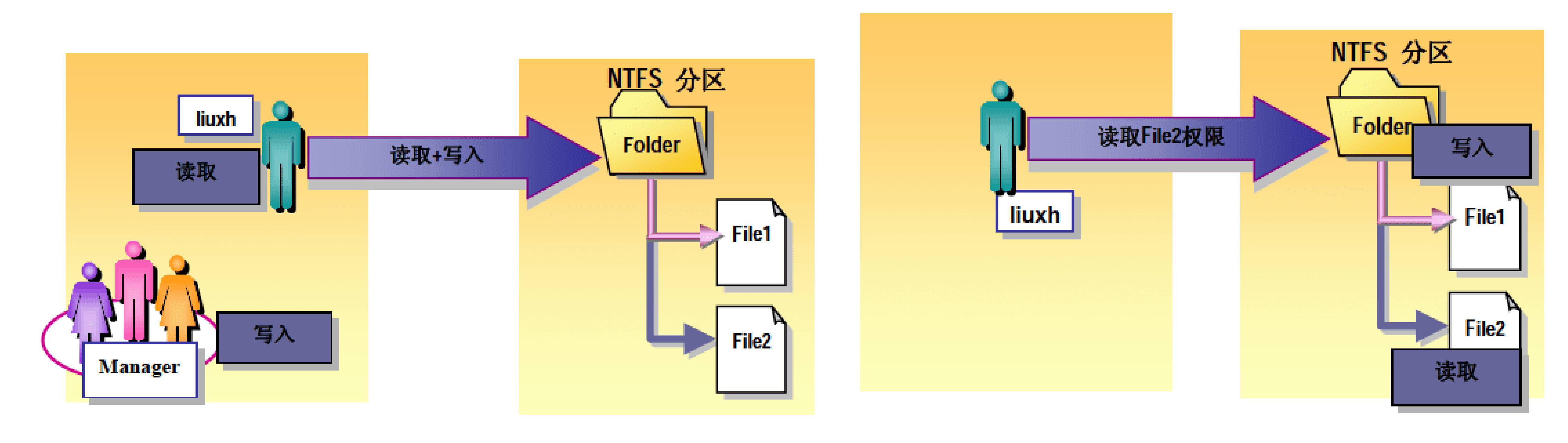


图 6-1 权限是累积的　　　　图 6-2 文件权限优先于文件夹权限

(3) 拒绝权限优先于其他权限

在 Windows 系统的所有 NTFS 权限中，拒绝权限优先于其他任何权限。即使用户作为一个组的成员有权访问文件或文件夹，一旦该用户被设置了拒绝访问权限，则最终将剥夺该用户可能拥有的任何其他权限。在实际使用中，应当尽量避免使用拒绝权限，因为允许用户和组进行某种访问，要比设置拒绝权限更容易做到。而事实上，只需巧妙地构造组和灵活组织文件夹中的资源，即可通过各种各样的“允许”权限满足访问控制的需求。

例如，User1 同时属于 Group B 组和 Group A 组。其中，User1 拥有对 Folder A 的读取权限，Group B 拥有对 Folder A 的读取和写入权限，Group A 则被禁止对 File2 的写操作。因此，User1 拥有对 Folder A 和 File1 的读取和写入权限，但对 File2 只有读取权限，如图 6-3 所示。

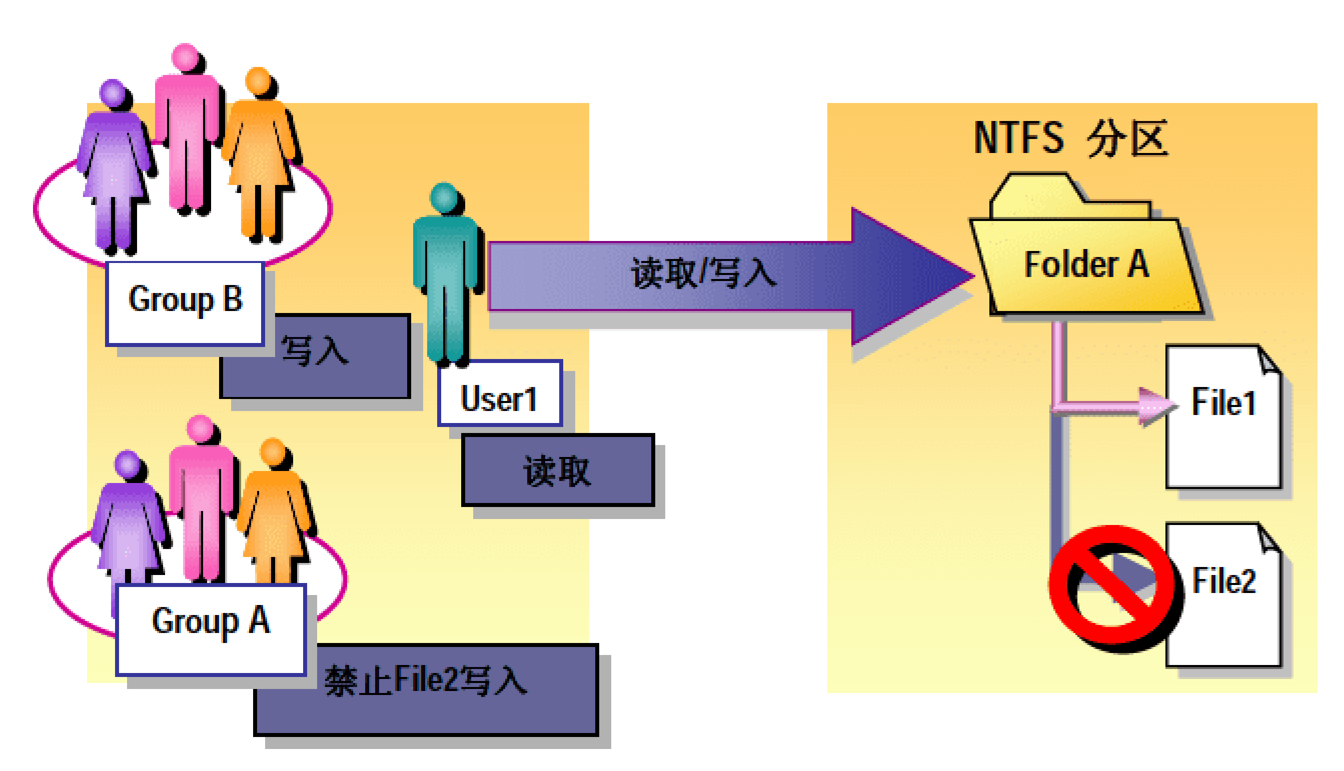


图 6-3 拒绝权限优先于其他权限

4. NTFS 权限的继承性

默认情况下，NTFS 权限是具有继承性的。所谓继承性，就是指 NTFS 权限自动从父对象传播到当前对象的过程，例如子文件夹继承来自其父文件夹的 NTFS 权限，文件继承来自文件夹的 NTFS 权限等。当然，正是因为 Windows 系统默认启用了 NTFS 权限继承，才会使用户不容易更加直观的判断对象最终的 NTFS 权限值。管理员可以根据实际情况，限制这种权限继承。

(1)　权限继承

文件和子文件夹从其父文件夹继承权限，即管理员为父文件夹指定的任何权限，同时也适用于在该父文件夹中所包含的子文件夹和文件。当为一个 NTFS 文件夹指定权限时，不仅为该文件夹及其中所包含的文件和子文件夹指定了权限，同时也为将来在该文件夹中创建的所有新文件和文件夹指定了权限。默认情况下，所有文件夹和文件都会自动从其父文件夹继承权限。

例如，当允许权限继承时，为 Folder1 设置的访问权限，将自动被传递给 File1、Folder2 和 File2。也就是说，子文件夹 Folder2 和文件 File1、File2 将自动取得为父文件夹 Folder1 设置的访问权限，如图 6-4 所示。

(2)　禁止权限继承

可以禁止指定给一个父文件夹的权限被这个文件夹中所包含的子文件夹和文件继承。也就是说，子文件夹和文件不会继承指定给包含它们的父文件夹的权限。被禁止继承权限的文件夹变成新的父文件夹，为该文件夹指定的权限将会被它所包含的任何子文件夹和文件继承。

例如，当禁止权限继承时，为 Folder1 设置的访问权限，将不被传递给 File1、Folder2 和 File2。也就是说，子文件夹 Folder2 和文件 File1、File2 不能自动取得为父文件夹 Folder1 设置的访问权限，必须为这些子文件夹和文件分别设置访问权限，如图 6-5 所示。

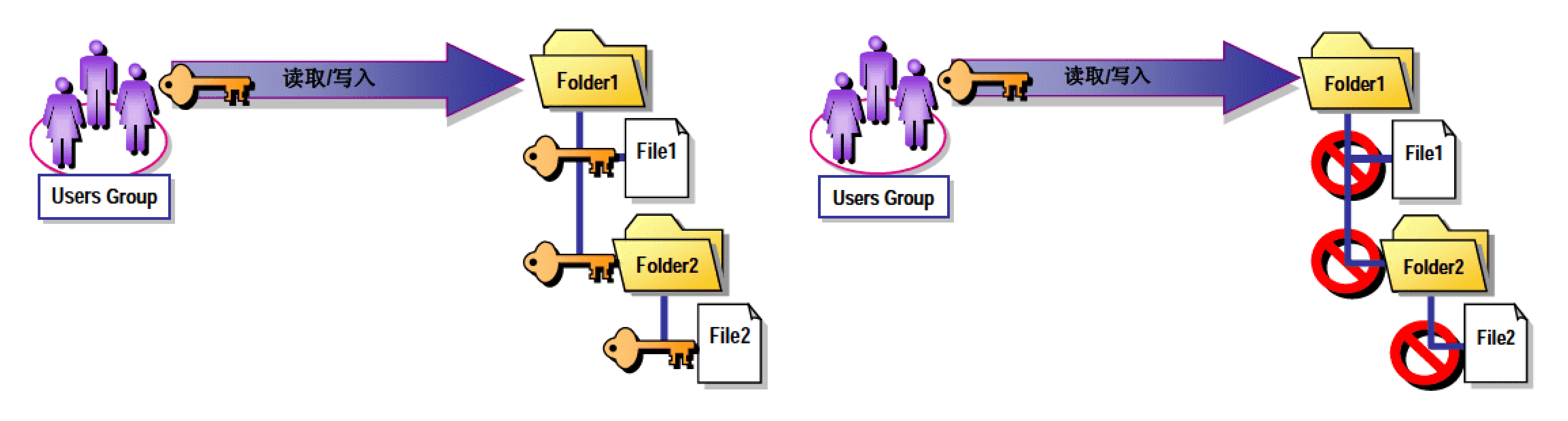


图 6-4　权限继承　　　　图 6-5　禁止权限继承

6.1.2　设置 NTFS 权限

NTFS 权限不仅在本地系统或本地域中有效，当目标资源在网络上共享时，这些权限设置同样有效，并且优先级高于共享权限设置。因此，从网络安全角度考虑，将资源设置为共享之前，应先配置其 NTFS 权限，以确保访问的安全性。

1. 设置 NTFS 权限基本策略和规则

在设置 NTFS 权限时，必须遵循以下基本策略和规则：

- 为了简化管理，应事先对目标文件进行分类管理，将同一类别归于同一文件夹中，例如可以分为应用程序、数据和主目录文件夹等，并将主目录和公共文件夹集中在一个与应用程序和操作系统分开的独立卷上，从而只需为文件夹指定权限，而不必为单独的文件指定权限。另外，将所有历史数据保存在同一目录下，还减少了备份工作的复杂性。
- 在文件夹级指定需要的全部权限，而不是在文件级指定权限。对于希望限制用户访问的文件用单独的文件夹将文件分组，然后为该文件夹指定受限制的访问权限。
- 只允许用户拥有他们所需要的存取级别，也就是说，为用户或用户组指定最严格的 NTFS 权限，只要能够完成所需的任务即可，从而减少用户意外修改或删除重要文档和程序文件的可能性。如果用户只需要读取一个文件，那么，就只赋予其对该文件的读取权限。
- 按照组成员对资源的访问需要创建组，然后，为组指定适当的权限。只有必要时才为单独的用户指定权限。
- 对于全部应用程序的可执行文件，应当为 Administrators 组指定读取、执行权限和更改权限，但只为 Users 组指定读取和执行权限，从而有效防止应用程序文件被删除或破坏。
- 对于公共数据文件夹，应当为 Creator Owner 指定完全控制权限，使用户可以删除和修改其创建的文件和文件夹，从而完全访问在公共数据文件夹中创建的文件或文件夹。
- 对于公共文件夹，应当为 Everyone 组指定读取权限和写入权限，并为 Creator Owner 指定完全控制权限，使用户能够完全访问他们创建的文件，读取和修改其他用户创建的文件，并能够读取、修改和删除他们自己创建的文件和文件夹。同时，Everyone 组的成员只能读取该文件夹中的文件，并可向该文件夹中添加文件。
- 设置允许权限而不是拒绝权限。如果不希望让某个用户或用户组访问某个特定的文件夹或文件，就不要为其指定权限。拒绝权限应当是个例外，而不是经常使用的操作。只有在必须拒绝特定的用户账户或组的某种特定的访问类型时，才设置拒绝权限。
- 如果只是在这台计算机上访问资源，则使用描述性的长文件名。如果该文件夹将来要共享，则使用可被所有客户计算机访问的文件夹和文件名，建议采用短文件名的格式。

借助于文件服务器中设置的访问控制列表(ACL)，不仅可以最大限度地保障重要数据存储安全，保证数据不会由于计算机的硬件故障而丢失，而且还可以通过严格的权限设置，有效地保证数据的访问安全。

网络攻击的目的在于获取用户权限，而获取用户权限的目的，在于获取超级文件权限。因此，做好文件权限的访问控制，才是最重要和最有效的安全措施。

2. 设置 NTFS 文件夹和文件权限

设置 NTFS 文件夹访问权限的主要操作步骤如下：

① 以管理员账户登录系统，打开 Windows 资源管理器，右击欲设置 NTFS 权限的文件夹(本例以 test 文件夹为例)，并选择快捷菜单中的“属性”命令，打开“test 属性”对话框，切换至如图 6-6 所示的“安全”选项卡。

② 在“组或用户名”列表框中选择想要配置权限的用户账户，如 hstjl，在下面的权限列表框中即可查看其当前权限。单击“编辑”按钮，显示如图 6-7 所示的对话框。继续在“组或用户名”列表框中选择 hstjl，即可在下面的“hstjl 的权限”列表框中修改其权限。默认情况下，是没有对普通用户设置任何 NTFS 访问权限的，用户账户将自动继承来自其所属组的权限，文件夹将自动继承来自其父文件夹的 NTFS 权限。

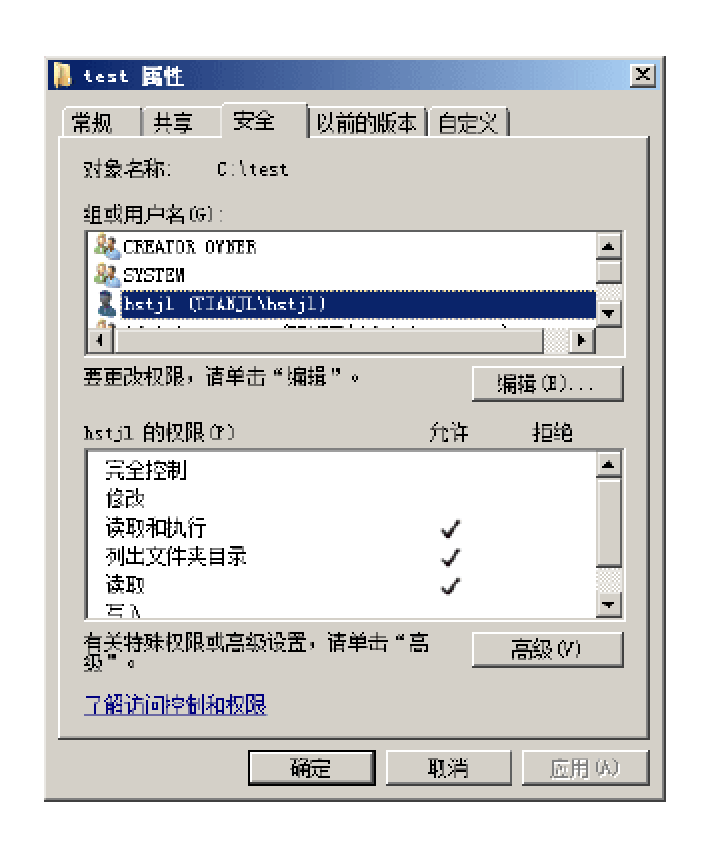


图 6-6　“安全”选项卡



图 6-7　更改用户权限



提示：如果权限带阴影显示，说明这些权限是从父文件夹的权限继承过来的。

③　如果“组和用户名”列表框中默认没有需要的用户账户，则可以单击“添加”按钮，显示如图 6-8 所示的“选择用户或组”对话框，在“输入对象名称来选择”文本框中，输入想要添加的用户账户名并单击“确定”按钮即可。在域控制器上还可以直接添加其他被信任域中的用户账户。

④　在更改用户权限对话框的“组或用户名”列表框中，选择想要删除的用户或组，并单击“删除”按钮，即可将其从列表框中删除。如果此时该账户所属组未被删除，则该账户仍具有相应访问权限。

⑤　单击“应用”和“确定”按钮，保存设置即可。重复上述操作，可以为不同用户账户指定不同的 NTFS 文件夹权限。

设置 NTFS 文件权限与设置 NTFS 文件夹权限非常相似，如图 6-9 所示，此处不再赘述。NTFS 文件权限仅对目标文件有效，但建议用户尽量不要采用直接为文件设置权限的方式，而应当将文件放置于文件夹中，然后对该文件夹设置权限。

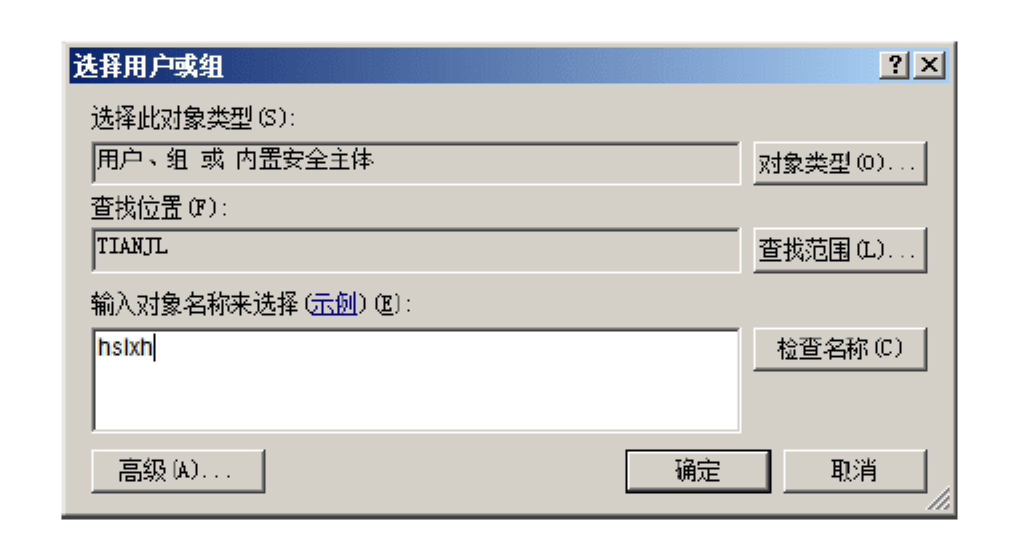


图 6-8　“选择用户或组”对话框

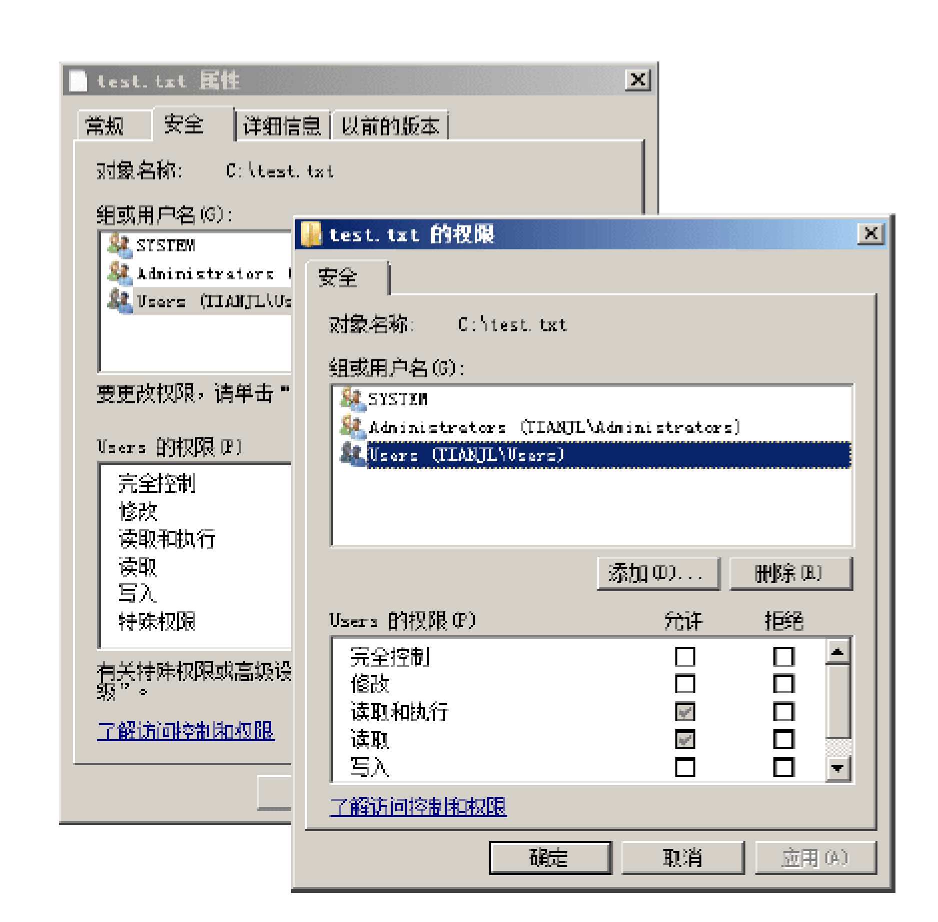


图 6-9　设置 NTFS 文件权限

3. 取消“Everyone”所有权限

Everyone 组是 Windows 系统中的一个特殊组，代表所有当前系统或网络上的所有用户账户，包括来自其他域或网络计算机的来宾账户，并且无论用户何时登录到网络上，或通过网络访问本地计算机，都会自动将该用户添加到 Everyone 组中。如果为 Everyone 组赋予某种控制权限，则任何用户都可以对所涉及的文件夹或文件进行操作，严重影响系统安全，因此建议取消 Everyone 组的所有权限。需要注意的是，在早期版本的 Windows NT 系统中，匿名登录用户也是属于 Everyone 组的，但在 Windows Server 2003/Windows Server 2008 系统中，“匿名登录”组在默认情况下已不是 Everyone 组的成员。

在资源管理器中，右击磁盘盘符，打开磁盘属性对话框，切换到“安全”选项卡，继续单击“编辑”按钮，显示如图 6-10 所示的对话框，在“组或用户名”列表框中选中 Everyone，并单击“删除”按钮将其删除。最后，单击“确定”按钮保存设置即可。

默认情况下，在 Windows Server 2008 系统中，Everyone 组只被赋予了很少的读取权限，安全性相对较高，但在早期版本的 Windows NT 系统中，该账户却拥有完全控制权限，很容易对系统安全造成威胁。

4. 指定高级访问权限

所谓高级权限主要是指系统默认赋予对象的，其默认设置为已被大多数用户所接受的权限，如权限继承就是其中的一种。高级访问权限主要为管理员提供更为详细的权限值设定，实现更加严格的网络安全管理。仍以 test 文件夹为例，设置高级权限的主要操作步骤如下。

① 在文件或文件夹属性的“安全”选项卡中，单击“高级”按钮，显示如图 6-11 所示的“test 的高级安全设置”对话框，默认只能查看每个用户账户的高级访问权限设置。

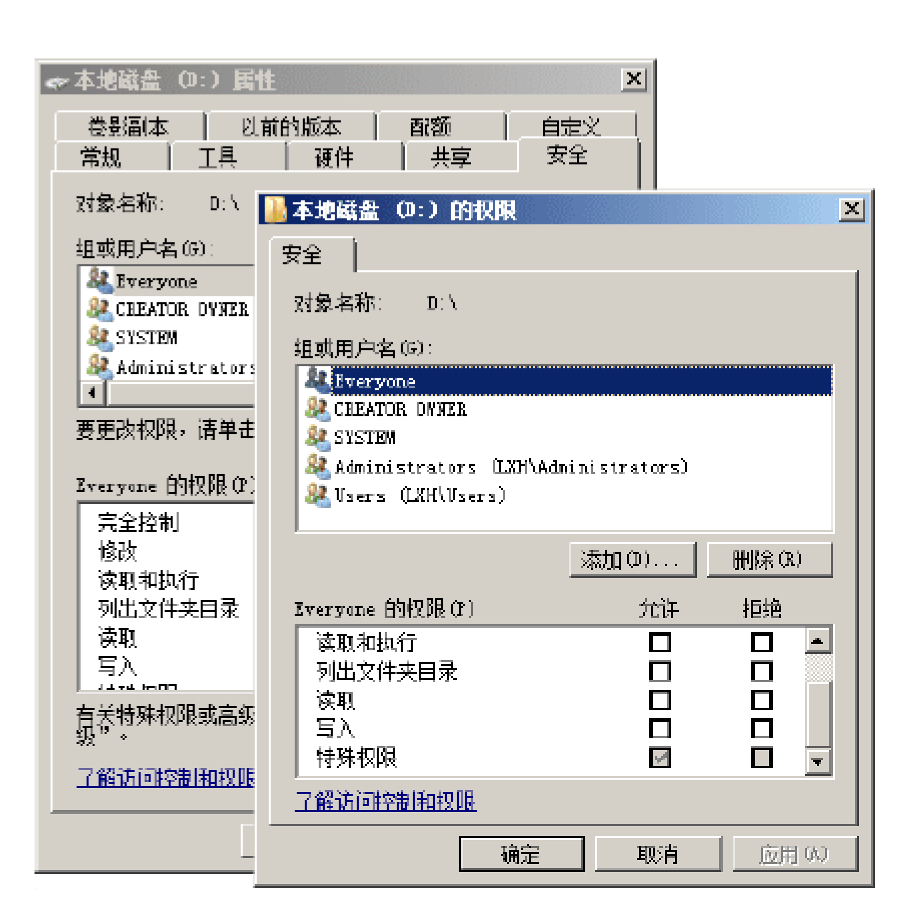


图 6-10　删除 Everyone 组

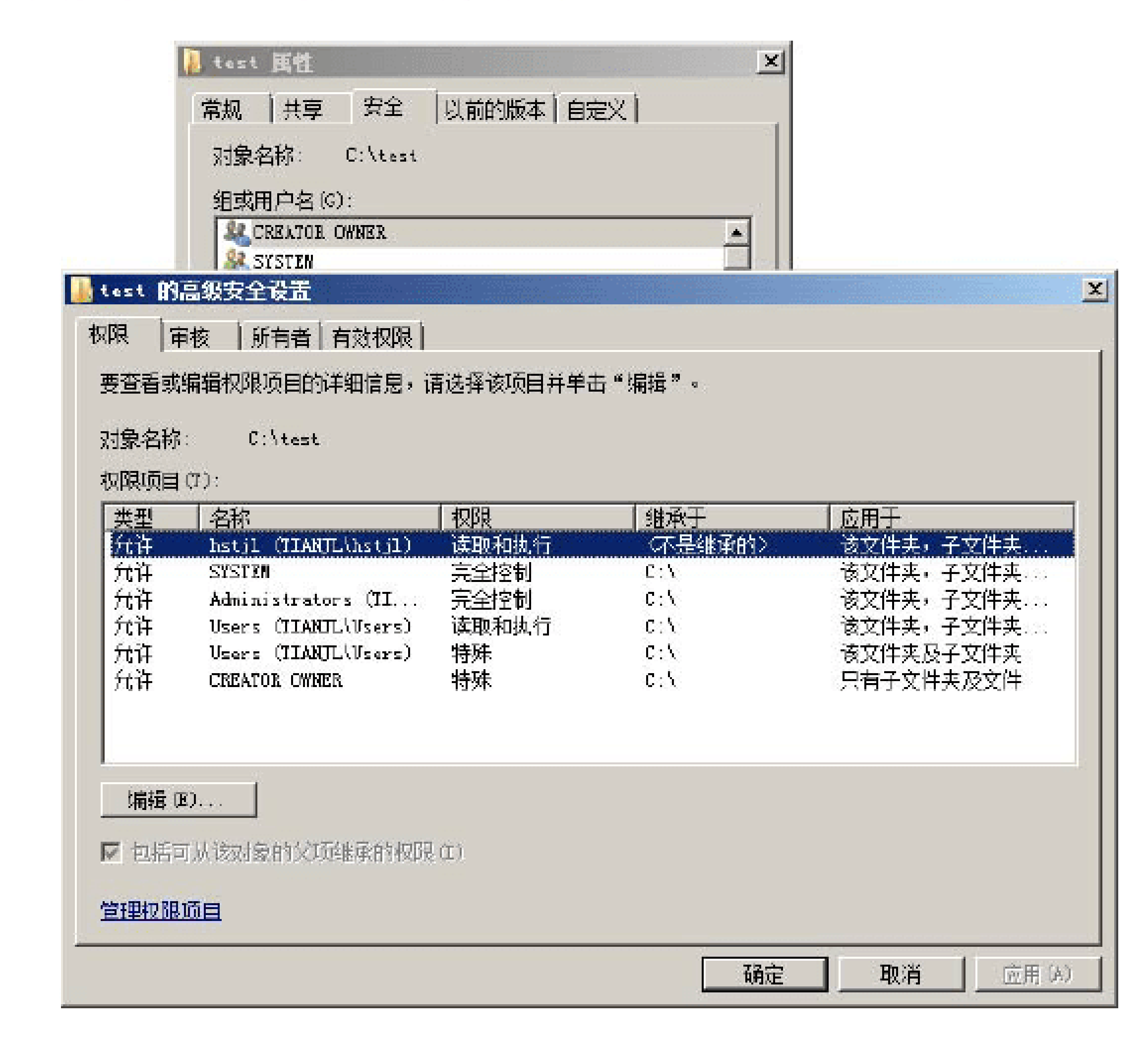


图 6-11　“test 的高级安全设置”对话框

② 在“权限项目”列表框中，选择想要设置高级权限的用户账户，如 hstjl。单击“编辑”按钮，显示如图 6-12 所示的对话框，用于设置高级权限。

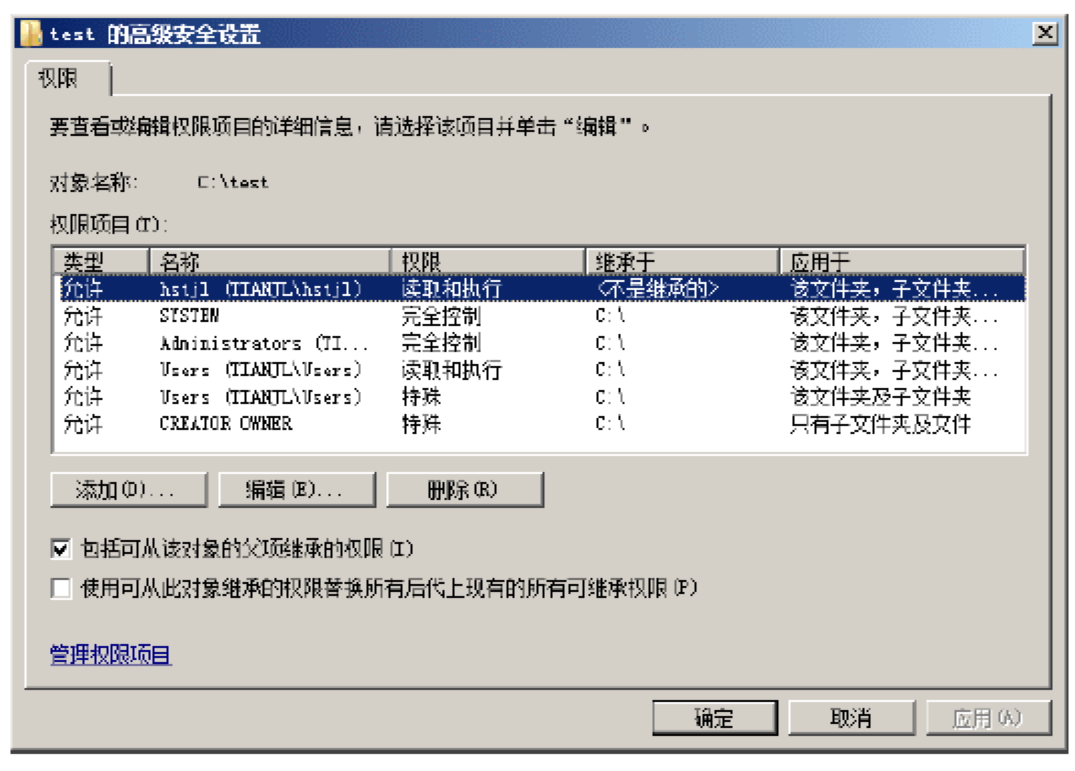


提示：系统默认已经选中“包括可从该对象的父项继承的权限”复选框，即自动继承来自父对象的高级权限，取消选中此复选框即可禁止 NTFS 权限的继承。



提示：选中“使用可从对象继承的权限替换所有后代上现有的所有可继承权限”复选框后，该父对象上的权限将替换其子对象上的权限；取消选中该复选框，则每个对象上的权限(无论是父对象还是子对象)都将是唯一的。

③　选择“权限项目”列表框中的 hstjl 账户，单击“编辑”按钮，显示如图 6-13 所示的“test 的权限项目”对话框。高级访问权限共有 14 项，组合在一起就构成了标准的 NTFS 权限。例如，标准的“读取”权限包含“读取数据”、“读取属性”、“读取权限”和“读取扩展属性”4 种特殊访问权限。



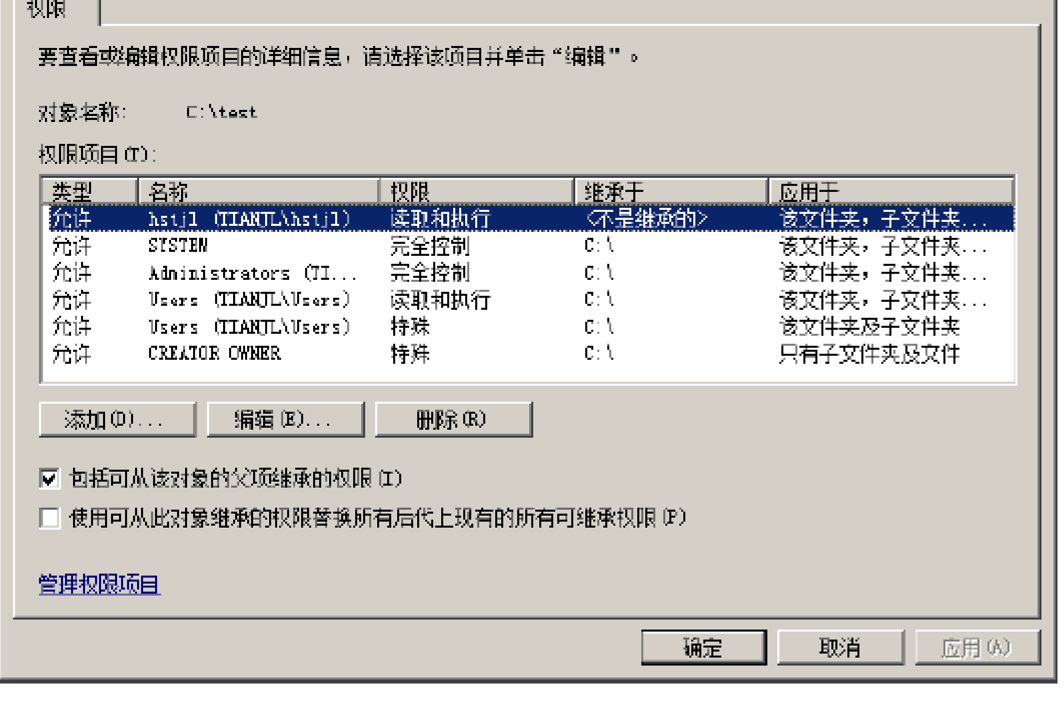


图 6-12　编辑高级权限

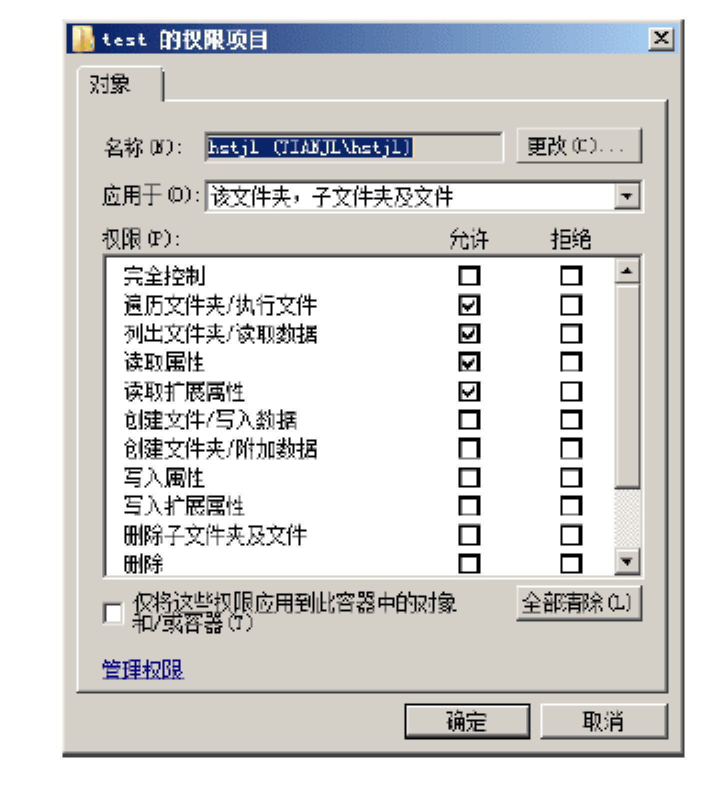


图 6-13　“test 的权限项目”对话框

有两个特殊访问权限对于管理文件和文件夹的访问者来说特别有用：

(1)　更改权限

被授予更改权限后，用户就具有了修改目标对象权限的权利。借助于更改权限，可以将针对某个文件或者文件夹修改权限的权利，授予其他管理员和用户，但是不授予他们对该文件或文件夹的“完全控制”权限。通过这种方式，这些管理员或者用户不能删除或者写入该文件或者文件夹，但可以为该文件或者文件夹授权。为了将修改权限的能力授予管理员，将针对该文件或者文件夹的“更改权限”授予 Administrators 组即可。

(2)　取得所有权

用户取得针对目标对象的所有权后，就具有了所有权利。借助于该权限，可以将文件和文件夹的拥有权从一个用户账户或者组转移到另一个用户账户或者组，也可以将“取得所有权”这种能力给予某个人，还可以获得某个文件或者文件夹的所有权。

在取得某个文件或者文件夹的所有权时，应当遵循以下规则：

- 当前的拥有者或者具有“完全控制”权限的任何用户，可以将“完全控制”这一标准权限或者“获得所有权”这一特殊访问权限授予另一个用户账户或者组。这样，该用户账户或者该组的成员就能获得所有权。
- Administrators 组的成员可以取得某个文件或者文件夹的所有权，而不管该文件夹或者文件授予了怎样的权限。如果某个管理员取得了所有权，则 Administrators 组也取得了所有权。因而该管理员组的任何成员都可以修改针对该文件或者文件夹的权限，并且可以将“取得所有权”这一权限授予另一个用户账户或者组。
- 为了成为某个文件或者文件夹的拥有者，具有“取得所有权”这一权限的某个用户或者组的成员，必须明确地取得该文件或者文件夹的所有权。不能自动将某个文件或者文件夹的所有权授予任何

一个人。文件的拥有者、管理员组的成员或者任何一个具有“完全控制”权限的人，都可以将“获得所有权”权限授予某个用户账户或者组，这样就使他们获得了所有权。

5. 复制和移动文件夹对权限的影响

在 NTFS 分区内和 NTFS 分区之间复制或者移动文件、文件夹时，Windows 系统会将其作为新文件或文件夹，因此，会对源文件或文件夹的 NTFS 权限产生影响。在复制文件和文件夹时，必须拥有源文件夹的“读取”权限，并且对目标文件夹具有“写入”权限。在移动文件或文件夹时，必须对目标文件夹拥有“写入”权限，并且对源文件夹拥有“修改”权限。

当从一个文件夹向另一个文件夹复制文件或文件夹时，或者从一个磁盘分区向另一个磁盘分区复制文件或文件夹时，复制文件或文件夹会对 NTFS 权限产生下述影响：

- 当在单个 NTFS 分区内复制文件夹或文件时，文件夹或文件的复制将继承目的文件夹的权限。
- 当在 NTFS 分区之间复制文件夹或文件时，文件夹或者文件的复件将继承目的文件夹的权限。
- 当将文件或文件夹复制到非 NTFS 分区(如 FAT32 分区或 FAT 分区)时，因为非 NTFS 分区不支持 NTFS 权限，所以，这些文件夹或文件将丢失 NTFS 权限。

移动对 NTFS 权限的影响如下：

- 当在单个 NTFS 分区内移动文件夹或文件时，该文件夹或者文件保留其原来的权限。
- 当在 NTFS 分区之间移动文件夹或文件时，该文件夹或文件将继承目的文件夹权限。当在 NTFS 分区之间移动文件夹或文件时，实际是将文件夹或文件复制到新位置，然后，将其从原来的位置删除。
- 当将文件或文件夹移动到非 NTFS 分区时，因为非 NTFS 分区不支持 NTFS 权限，所以，这些文件夹或文件将丢失其 NTFS 权限。

6.1.3 设置磁盘配额

磁盘配额是 NTFS 文件系统特有的安全功能，可以帮助管理员控制每个用户账户的磁盘空间使用情况。磁盘配额是以文件所有权为基础的，只应用于卷，且不受卷的文件夹结构及物理磁盘上的布局影响。由于磁盘配额监视个人用户卷的使用情况，因此，每个用户对磁盘空间的利用都不会影响同一卷上其他用户的磁盘配额。

1. 磁盘配额的功能

磁盘配额管理技术，主要是根据网络管理员设置的标准，跟踪对被保护卷的写操作，如果被保护卷达到或超过了设定级别，则用户就会收到服务器自动发送的消息，警告该卷已经接近配额，或者磁盘配额管理器将阻止用户向该卷写数据。管理员能够启用磁盘配额，并设置两个值：

- 磁盘配额限度。用于指定允许用户使用的磁盘空间容量。
- 磁盘配额警告级别。指定了用户接近其配额限度的值。

在 Windows Server 2008 系统中，管理员可以配置当用户超过所指定的磁盘空间限额时，阻止其进一步使用磁盘空间和记录事件，或当用户超过指定的磁盘空间警告级别时，记录事件。第一种配置情况下，用户在使用磁盘时如果超过指定的磁盘空间，将无法使用；第二种情况允许用户超额使用磁盘，但会将此情况记录在事件中。

同时可以指定用户能超过其配额的限度。如果不想拒绝用户访问卷但想跟踪每个用户的磁盘空间使用情况，启用配额但不限制磁盘空间使用将非常有用。也可指定不管用户超过配额警告级别还是超过配额限度时是否记录事件。

启用卷的磁盘配额时，磁盘配额不应用到现有的卷用户上。可以通过在“配额项目”窗口中添加新的配额项目将磁盘空间配额应用到现有的卷用户上。

由于磁盘配额能够监视单个用户的卷使用情况，因此每个用户对磁盘空间的利用都不会影响同一卷上的其他用户的磁盘配额。在用户看来与在一个独立的磁盘卷中进行操作没什么两样。

要支持磁盘配额，磁盘卷必须使用 NTFS 文件系统格式化，且不受卷中用户文件的文件夹位置的限制。

2. 磁盘配额管理

如果要在已经使用的磁盘中启用磁盘配额功能，Windows Server 2008 将计算到启动时间点为止，在该卷中复制文件、保存文件或取得文件所有权的所有用户使用的磁盘空间。根据统计结果，自动为每个用户设置配额限度和警告级别。当然，管理员可以为某个或多个用户设置不同的配额或禁用配额。另外，也可以为还没有在卷上复制文件、保存文件和取得文件所有权的用户设置磁盘配额，或者在一个新创建的卷上启用磁盘配额功能。

使用磁盘配额过程中，应注意以下 3 个方面：

- 驱动器的文件格式必须为 NTFS 文件系统格式。如果驱动器的磁盘格式为 FAT32 文件系统，可以使用 Windows Server 2003/2008 提供的文件系统转换工具 Convert 进行转换。
- 必须以管理员或管理员组成员的身份登录到 Windows 系统。
- 在文件服务器上选中“为此服务器的新用户设置默认磁盘空间配额”复选框，在“将磁盘空间限制为”和“将警告级别设置为”文本框中，输入适当的数值，使用户只能使用规定数额的磁盘空间，从而避免服务器硬盘的滥用。当用户使用的空间达到指定的警告值时，系统将提示用户磁盘空间剩余值。当用户使用的空间达到规定的磁盘限额时，系统将禁止用户再向服务器写入文件，从而确保服务器硬盘空间被合理、公平的使用。

(1) 启动磁盘限额

在默认的情况下，磁盘配额是没有启用的。启动磁盘配额的操作步骤如下。

① 在 Windows 资源管理器中，右击想要启用配额功能的 NTFS 卷(如本地磁盘 C:)，并选择快捷菜单中的“属性”命令，打开“本地磁盘(C:) 属性”对话框，切换到如图 6-14 所示的“配额”选项卡，选中“启用配额管理”复选框，即可启用磁盘配额管理。

选择其中相应的各个选项，以配置系统的磁盘配额功能：

- 选中“拒绝将磁盘空间给超过配额限制的用户”复选框，超过其配额限制的用户，将收到来自 Windows 的“磁盘空间不足”的错误信息，并且在没有从中删除和移动一些现存文件的情况下，无法将额外的数据写入卷中。如果取消选中该复选框，则用户可以超过其配额限制。
- 选择“将磁盘空间限制为”单选按钮，并输入允许卷的新用户使用的磁盘空间数量，以及在将事件写入系统日志前已经使用的磁盘空间量。网络管理员可以在“事件查看器”中查看这些事件。在磁盘空间和警告级别中可以使用十进制数值，从下拉列表框中选择适当的单位(如 KB、MB、GB 等)。
- 选中“用户超出配额限制时记录事件”复选框。此时如果启用配额，则只要用户超过其配额限制，事件就会写入到本地计算机的系统日志中。管理员可以用“事件查看器”，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

- 选中“用户超过警告等级时记录事件”复选框。此时如果启用配额，则只要用户超过其警告级别，事件就会写入到本地计算机的系统日志中。管理员可以用事件查看器，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

② 单击“确定”按钮，保存所做设置，启用磁盘配额完成。

③ 启用磁盘配额管理后，所有的用户都使用磁盘配额启动时设置的默认配额限制和配额警告级别。使用配额项目管理可以为每一个用户设置适合的磁盘配额，对用户的磁盘配额设置进行维护，并且可以记录每一个用户对磁盘空间的使用情况。

(2) 为特定的用户磁盘配额

若让某一个用户使用更多的空间，可以为该用户单独制定更大的磁盘配额。

① 在驱动器属性对话框中，切换到“配额”选项卡，单击“配额项”按钮，显示如图 6-15 所示的“(C:)的配额项”窗口。

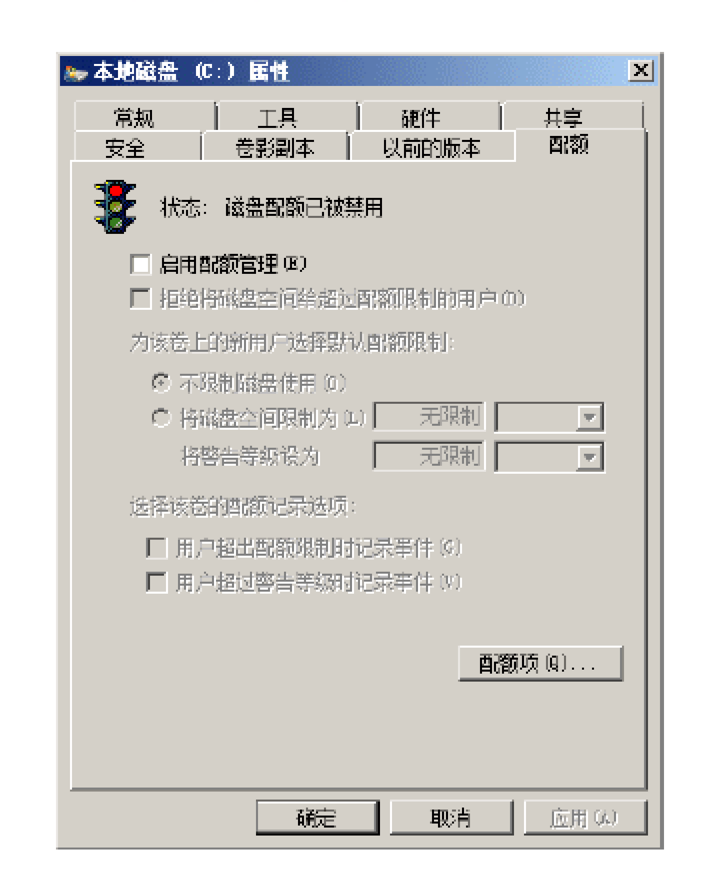


图 6-14 “配额”选项卡

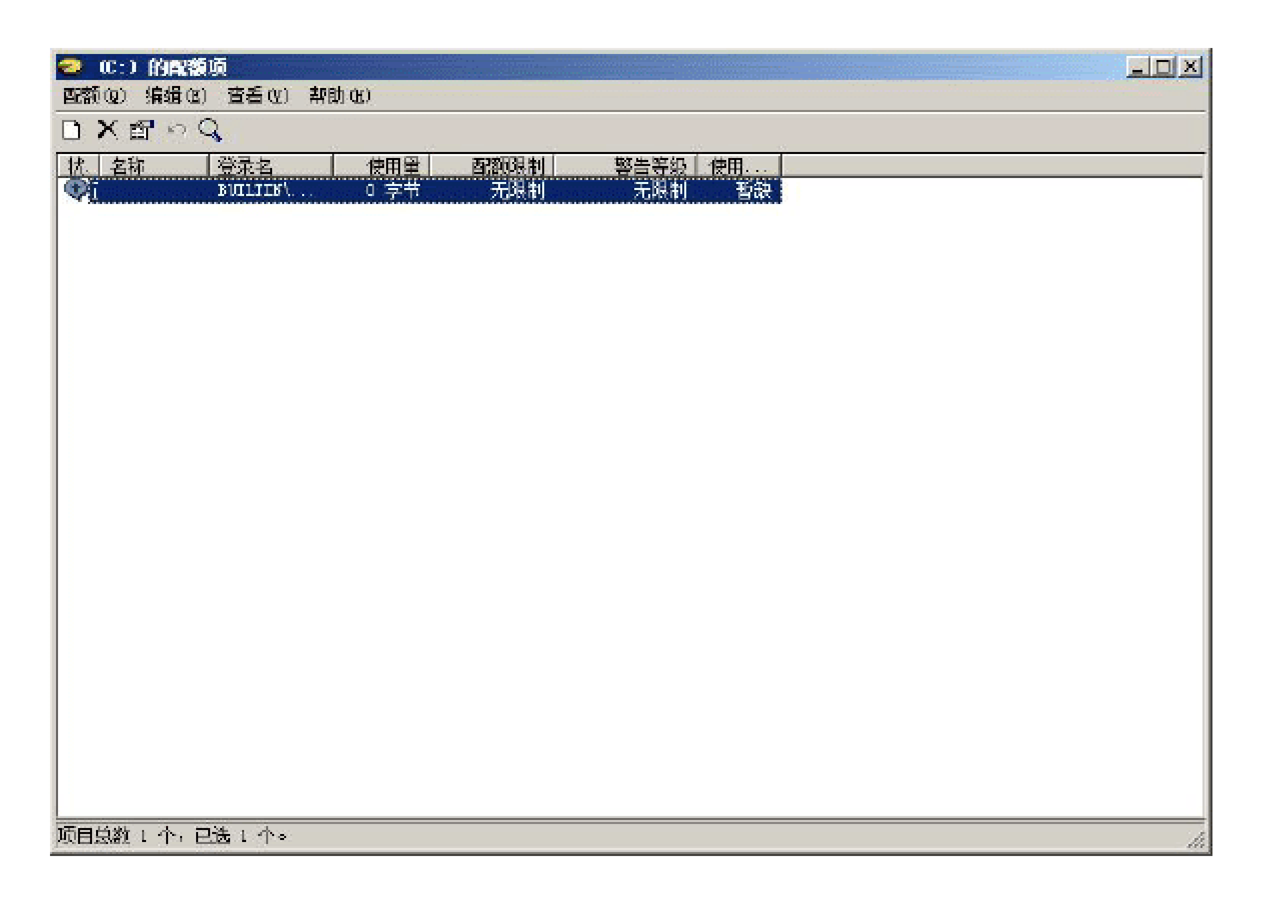


图 6-15 “(C:)的配额项”窗口

② 选择“配额”|“新建配额项”命令，或者单击工具栏中的“新建配额项”按钮，显示如图 6-16 所示的“选择用户”对话框。在“选择此对象类型”文本框中显示出当前的对象类型为“用户”，可采用系统的默认值。在“输入对象名称来选择”文本框中，输入要设置配额的用户名称。单击“检查名称”按钮，检查输入的用户账户是否存在。

③ 单击“确定”按钮，显示如图 6-17 所示的“添加新配额项”对话框。选择“将磁盘空间限制为”单选按钮，并在其后文本框中为该用户设置访问磁盘的空间。

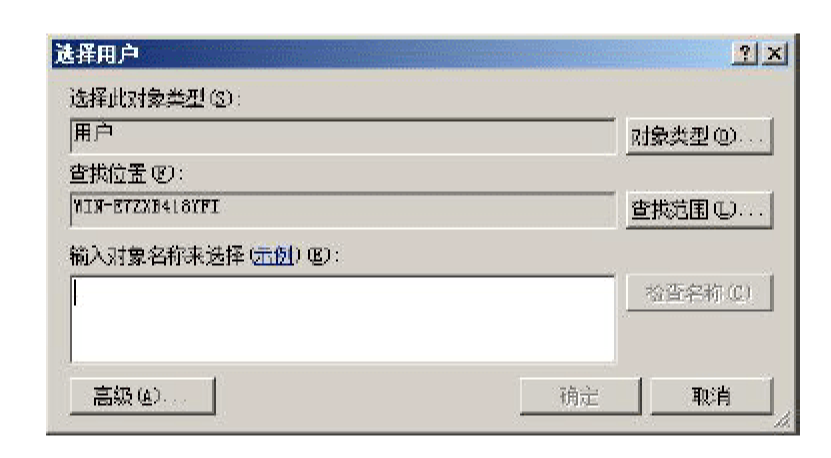


图 6-16 “选择用户”对话框

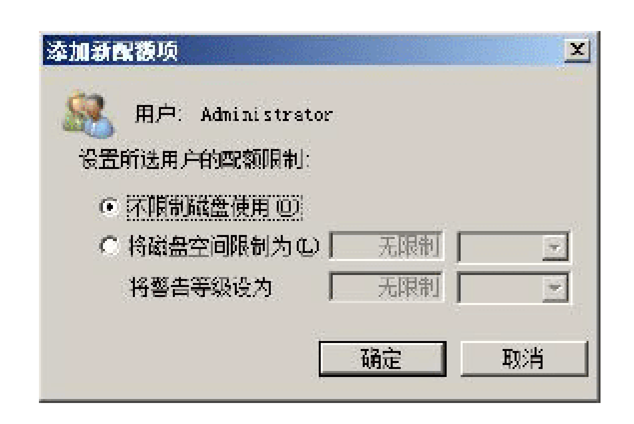


图 6-17 “添加新配额项”对话框

④ 单击“确定”按钮，保存用户的磁盘配额设置，返回到“(C:)的配额项目”窗口，可以看到新创建的用户 Administrator 配额项显示在列表框中。

如果想删除指定用户的配额项，可选择用户名，右击并选择快捷菜单中的“删除”命令即可。

使用指定配额项具有以下几个优点：

- 登录到相同计算机的多个用户之间互不影响。
- 一个或多个用户不独占公用服务器上的磁盘空间。
- 在个人计算机的共享文件夹中，用户不使用过多的磁盘空间。

3. 监控每个用户的磁盘配额使用情况

当为用户设置好磁盘配额以后，除了可以借助“日志查看器”浏览磁盘占用情况外，在配额项窗口中，也可以监视每个用户的磁盘配额使用情况，并可单独设置每个用户可使用的磁盘空间。也就是说配额项的主界面就是一个用户配额监控器。

如果要更改某一个用户的磁盘配额设置，可右击该用户，选择快捷菜单中的“属性”命令，显示如图 6-18 所示的配额设置对话框，可以更改用户的磁盘空间限制及警告等级。

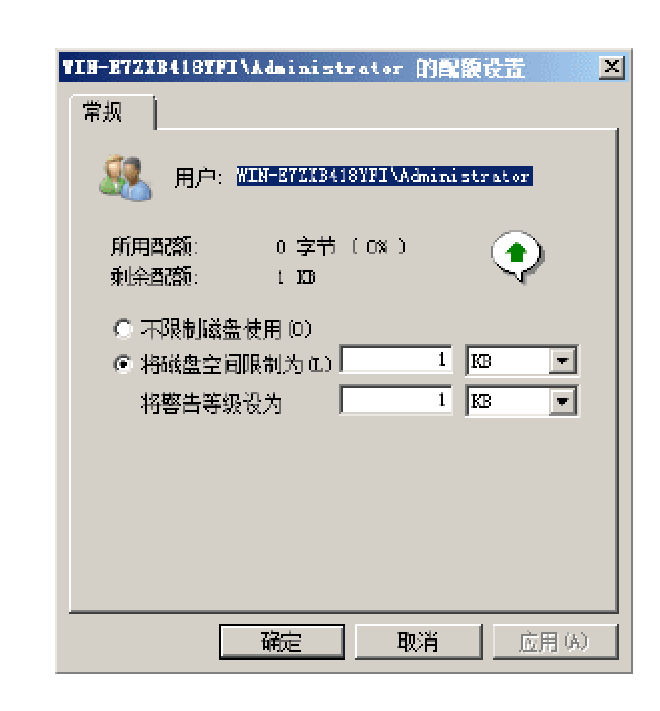


图 6-18　配额设置对话框

6.1.4　文件屏蔽

文件屏蔽是文件服务器中的重要功能，部署文件服务器之后，即可使用该功能限制用户向文件服务器写入的文件类型。任何用户将限制类型的文件写入目标文件夹时，都将出现“目标文件夹访问被拒绝”的信息。文件屏蔽的主要目的是限制非法授权文件写入定义的文件夹。

1. 创建限制文件组

限制文件组，就是定义需要限制的文件类型，支持通配符(*、?等)定义。文件服务安装完成后，预定义了 11 个文件组。本例屏蔽除文本文件外的所有文件类型。

① 依次选择“开始”→“管理工具”→“文件服务器资源管理器”选项，打开“文件服务器资源管理器”窗口，依次展开“文件屏蔽管理”→“文件组”，显示如图 6-19 所示的窗口。

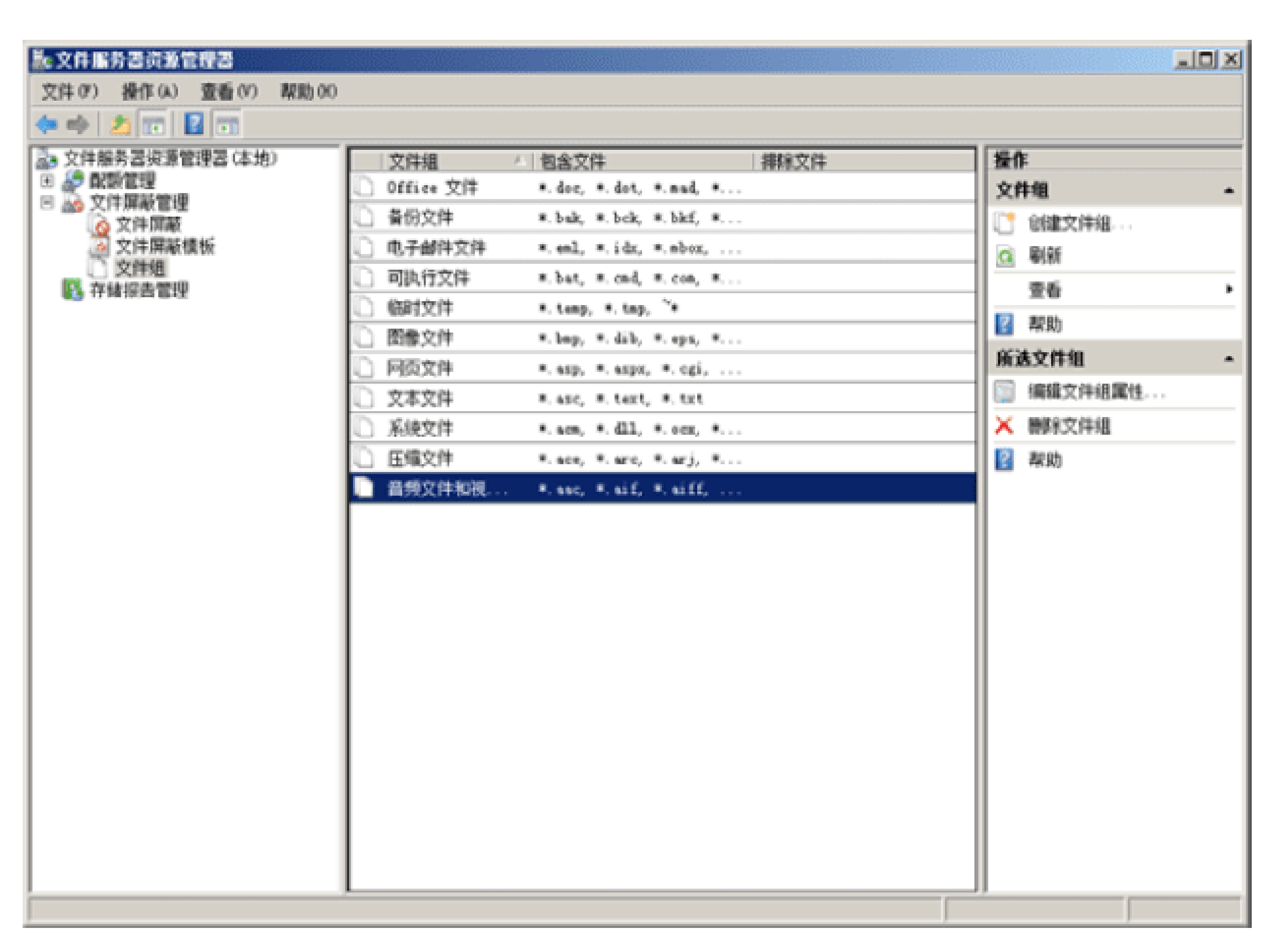


图 6-19　“文件服务器资源管理器”窗口

② 右击“文件组”，在弹出的快捷菜单中选择“创建文件组”命令，显示如图 6-20 所示的“创建文件组属性”对话框。在“文件组名”文本框中输入新文件组的名称；在“要包含的文件”文本框中，输入“*.*”，表示当前策略关联所有类型的文件。

③ 单击“添加”按钮，将“*.*”加入到文件列表框中。如需排除某种类型的文件，可以在“要排除的文件”文本框中输入对应文件的扩展名(如*.txt)，然后单击其右侧的“添加”按钮，将其加入到文件列表框中，如图 6-21 所示。

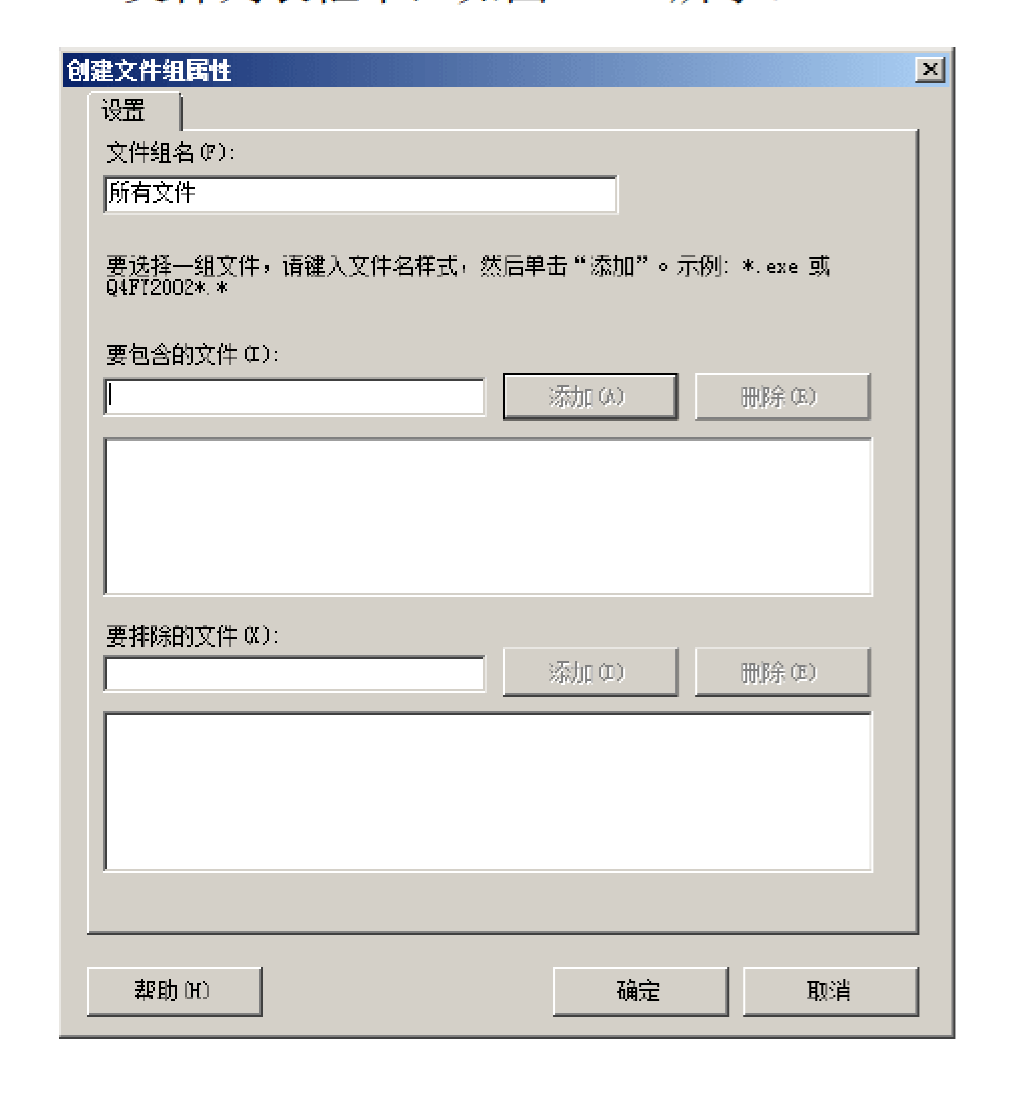


图 6-20 “创建文件组属性”对话框

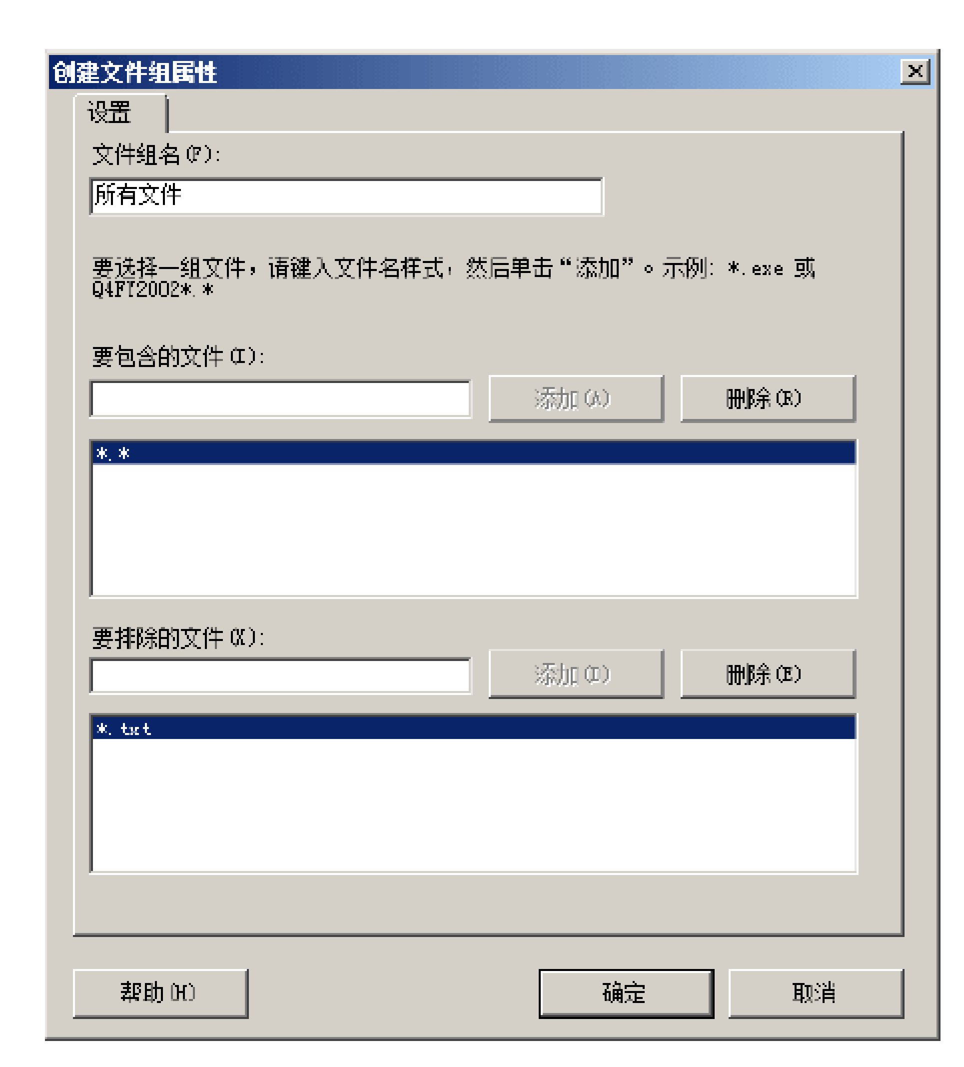


图 6-21 添加文件类型

④ 单击“确定”按钮，完成新文件组的创建，如图 6-22 所示。

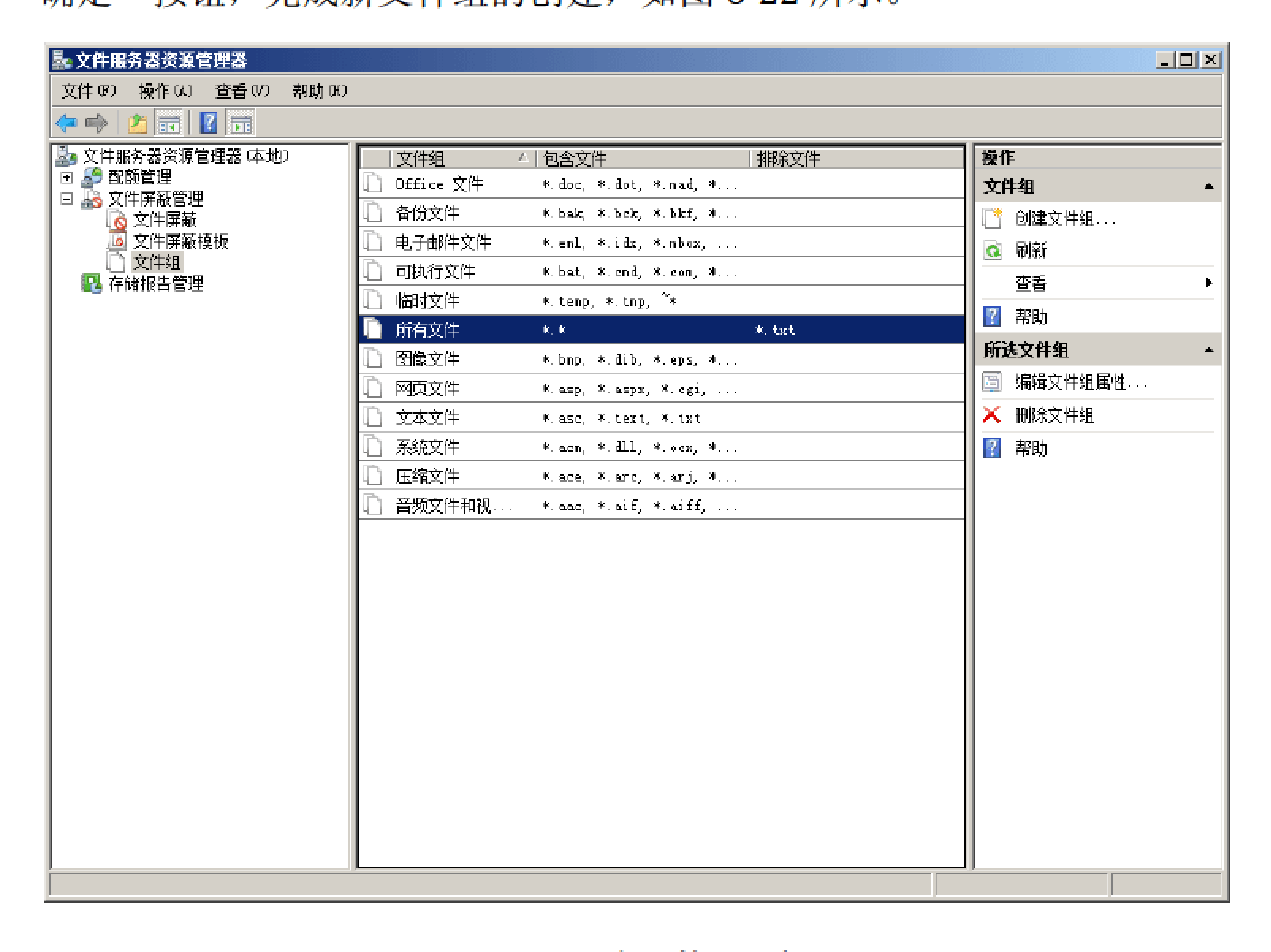


图 6-22 服务器管理器窗口

2. 创建屏蔽模板

屏蔽模板，定义文件组被监控以及监控方式，提供主动屏蔽和被动屏蔽两种模式。主动屏蔽，将屏蔽文件组中定义的文件类型关联的文件；被动屏蔽，仅监控文件组中定义的文件，但不限制写入目标文件夹。

① 在“文件服务器资源管理器”窗口中，展开如图 6-23 所示的“文件屏蔽模板”选项。文件服务安装完成后，默认已经预定义了 5 个文件屏蔽模板。

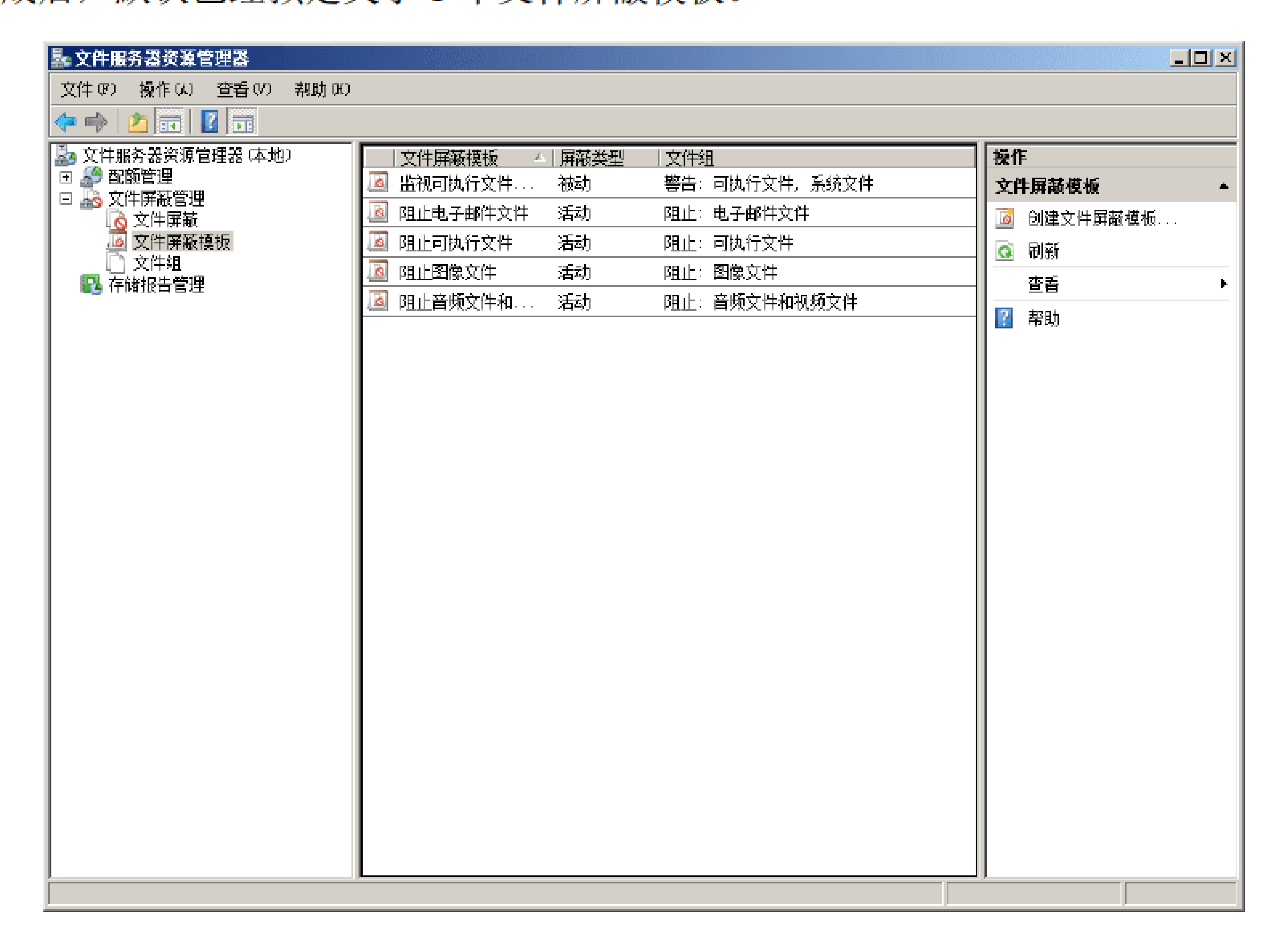
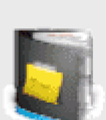


图 6-23　“文件屏蔽模板”窗口

② 右击“文件屏蔽模板”，选择快捷菜单中的“创建文件屏蔽模板”命令，显示如图 6-24 所示的“创建文件屏蔽模板”对话框。在“模板名”文本框中，输入新模板的名称；选择“主动屏蔽”单选按钮；在“选择要阻止的文件组”列表框中选择需要主动屏蔽的文件组，本例中选择新创建的“所有文件”文件组。



提示：“主动屏蔽”和“被动屏蔽”的主要区别在于：“主动屏蔽”屏蔽符合文件组设置的所有文件；“被动屏蔽”监控用户保存到目标文件夹的文件，可以正常写入，仅提供报警功能。

③ 单击“确定”按钮，显示如图 6-25 所示的“更新从模板派生的文件屏蔽”对话框，选择“仅将模板应用于与原始模板匹配的派生文件屏蔽”单选按钮。

④ 单击“确定”按钮，完成屏蔽模板的创建，如图 6-26 所示。

3. 部署文件屏蔽策略

部署文件屏蔽策略的方法很简单，选择目标文件夹后，将创建的文件屏蔽模板绑定到目标文件夹即可。

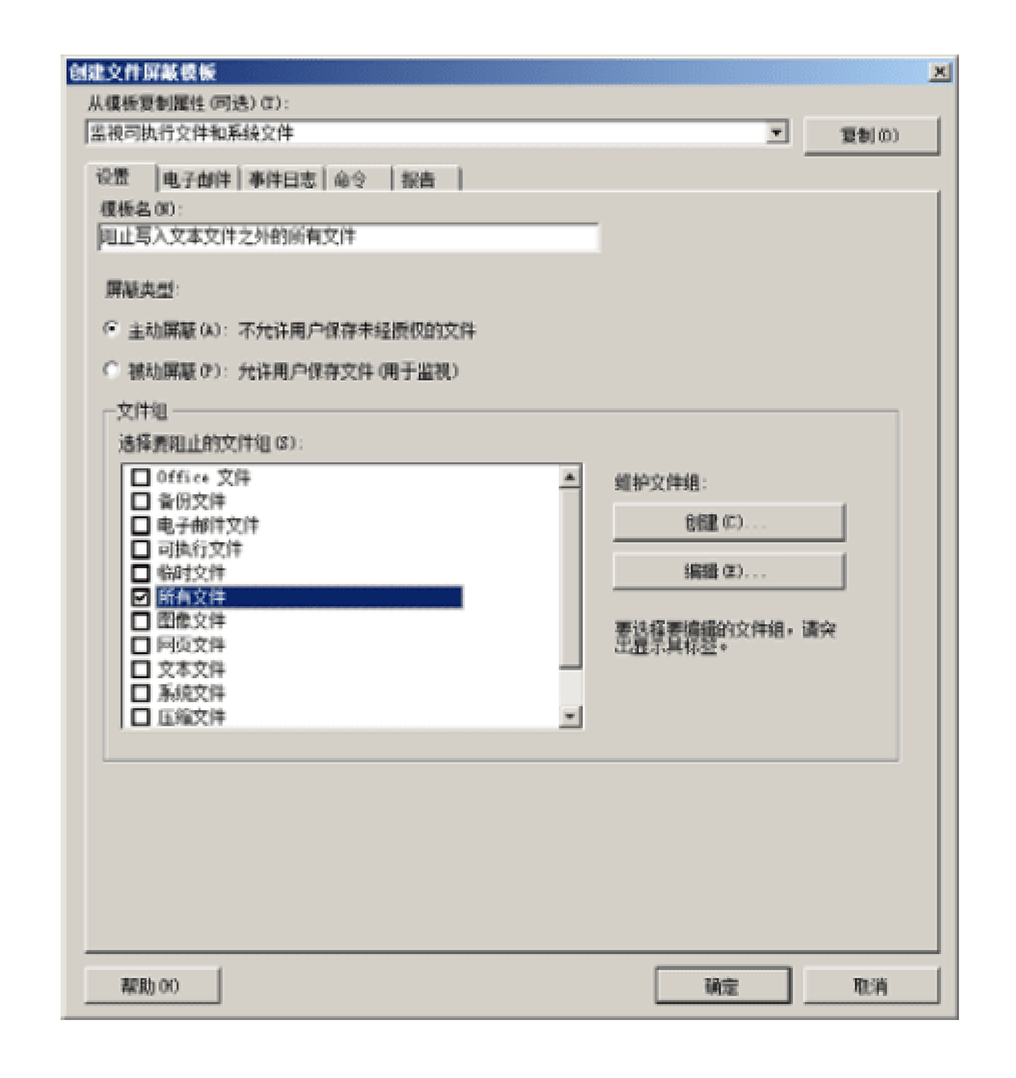


图 6-24 “创建文件屏蔽模板”对话框

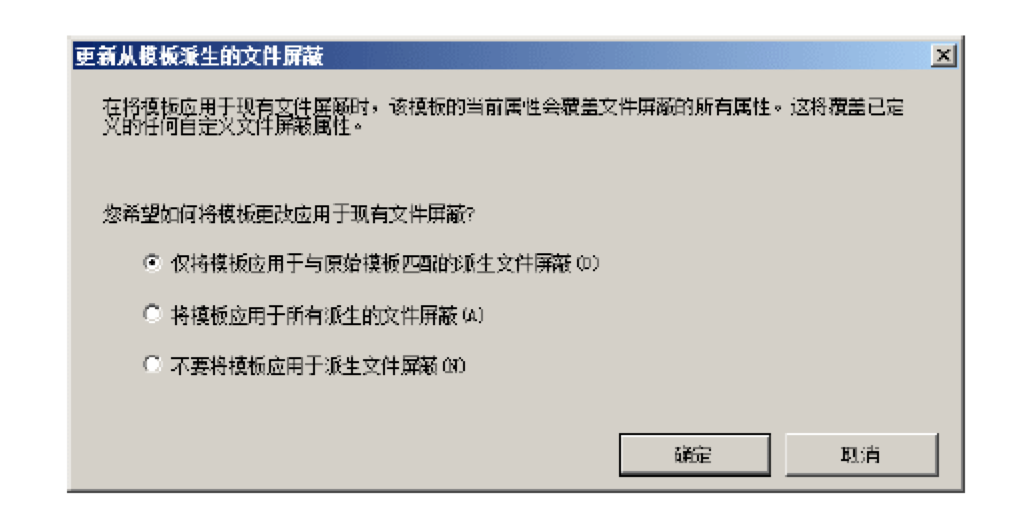


图 6-25 “更新从模板派生的文件屏蔽”对话框

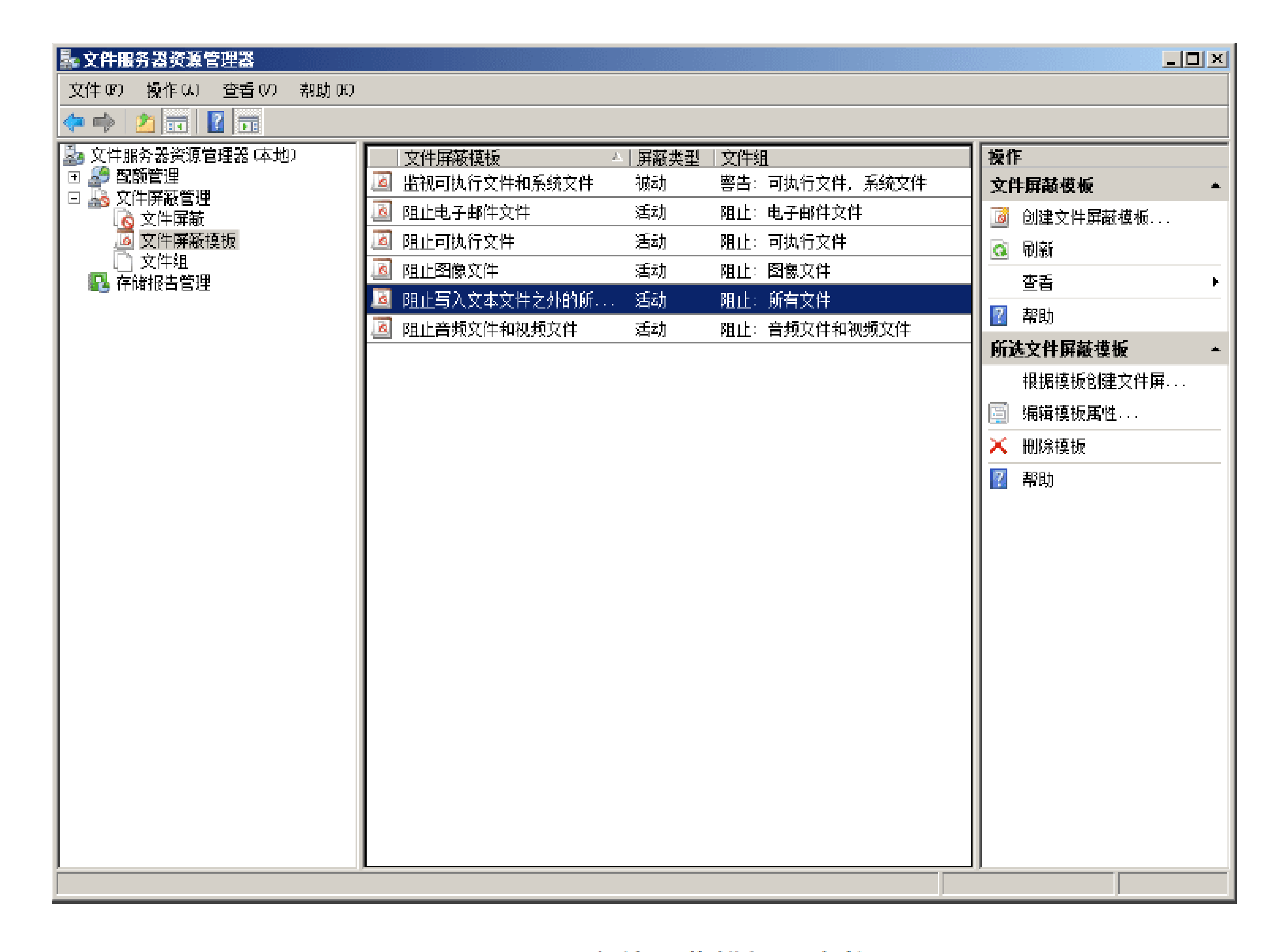


图 6-26 “文件屏蔽模板”窗格

① 在“文件服务器资源管理器”窗口中，右击“文件屏蔽”并选择快捷菜单中的“创建文件屏蔽”命令，显示如图 6-27 所示的“创建文件屏蔽”对话框。

② 单击“浏览”按钮，显示如图 6-28 所示的“浏览文件夹”对话框。在“选择文件夹”列表框中，选择需要保护的目标文件夹。

③ 单击“确定”按钮，返回到“创建文件屏蔽”对话框。在“文件屏蔽属性”选项区域的“从此文件屏蔽模板派生属性”下拉列表框中，选择“阻止写入文本文件之外的所有文件”选项，在“文件屏蔽属性摘要”文本框中即可显示该屏蔽模板的详细信息，如图 6-29 所示。

④ 单击“创建”按钮，创建新的文件屏蔽策略，创建完成的策略如图 6-30 所示。

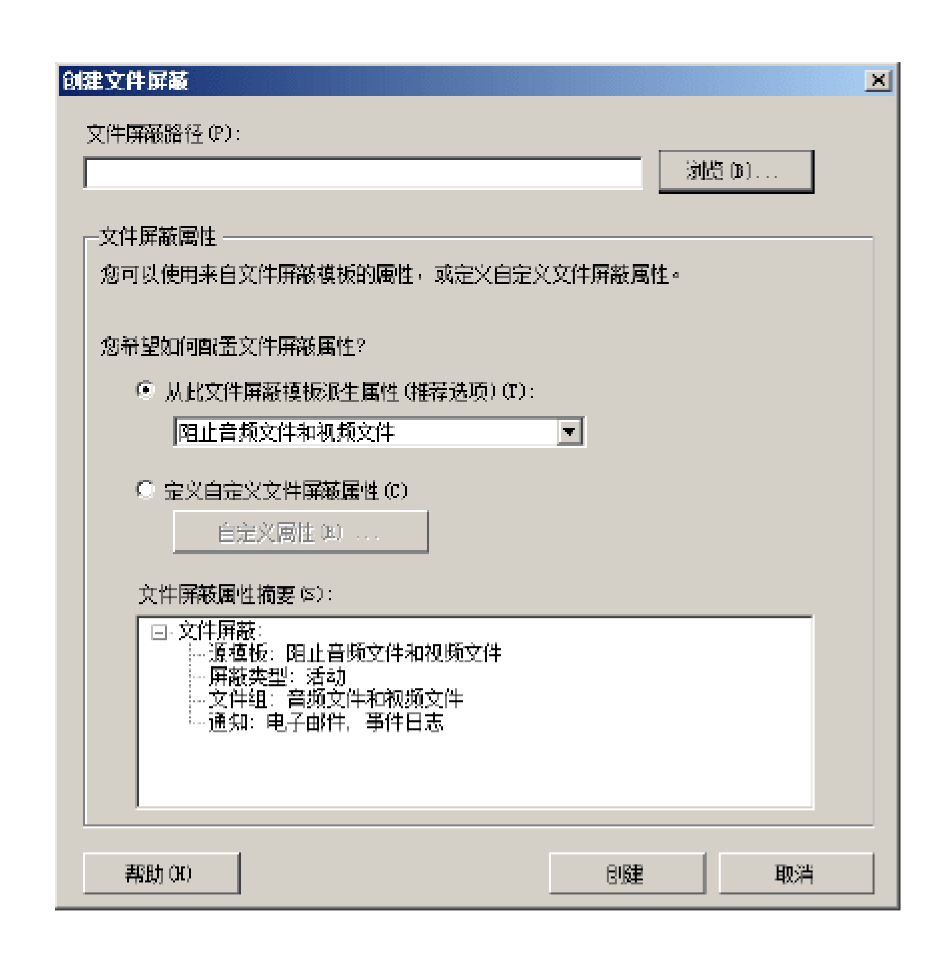


图 6-27　“创建文件屏蔽”对话框

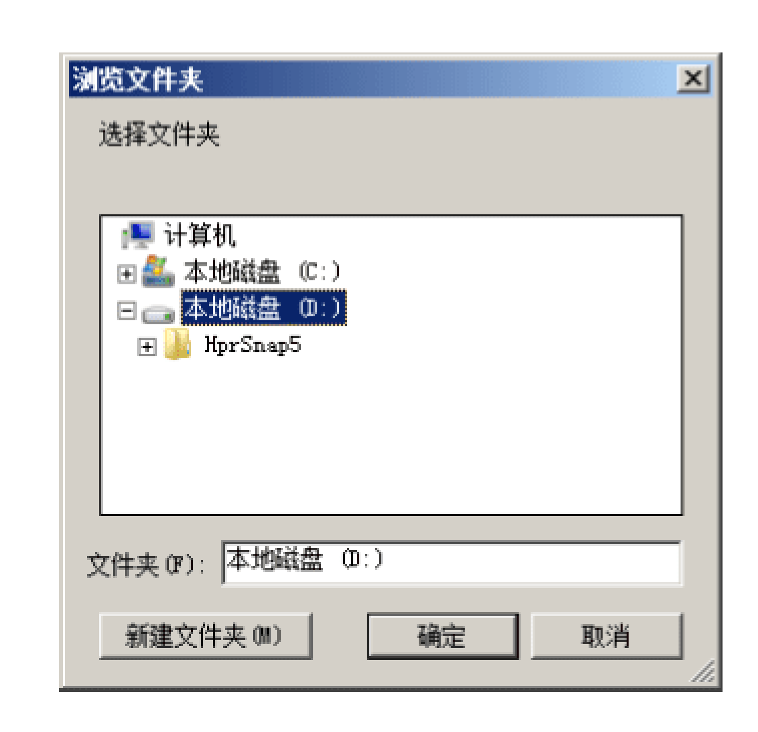


图 6-28　“浏览文件夹”对话框

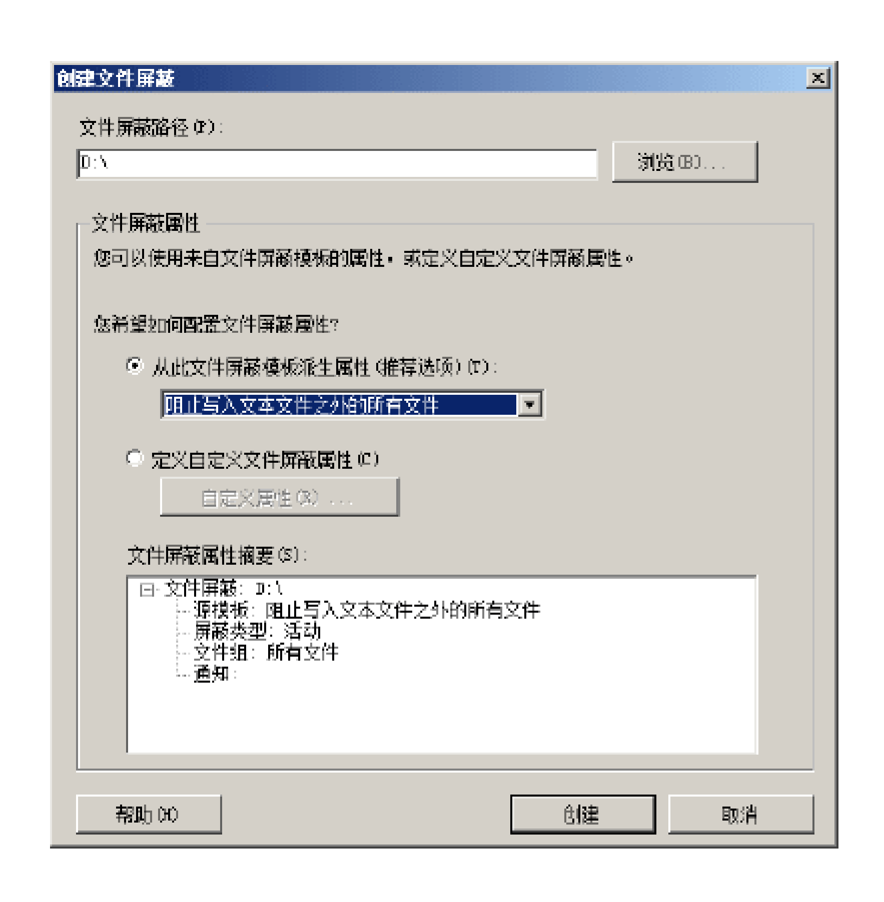


图 6-29　“创建文件屏蔽”对话框

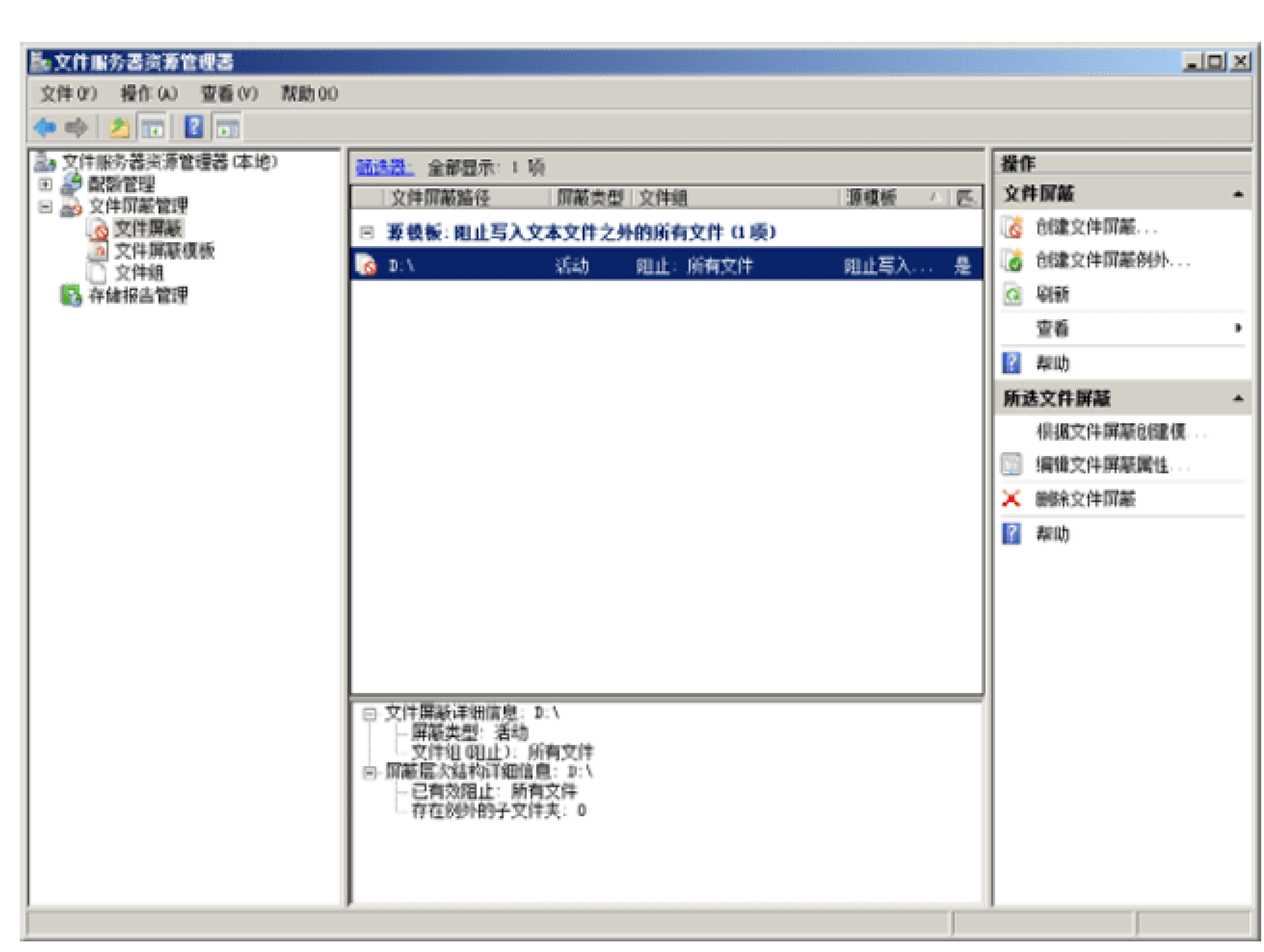


图 6-30　“文件屏蔽”窗格

4. 文件屏蔽测试

此时文件屏蔽模板的内容是：阻止写入文本文件之外的所有文件。为了验证设置是否生效，可以进行如下试验。

① 在受保护的目录下（本例中为 D:\）新建一个.docx 文件时，显示如图 6-31 所示的“目标文件夹访问被拒绝”对话框，.docx 类型的文档不能创建。

② 仍在该目录下，新建一个.txt 文件时，可以顺利完成，如图 6-32 所示。这是因为屏蔽文件类型中已经排除了“*.txt”文件。



图 6-31　“目标文件夹访问被拒绝”对话框

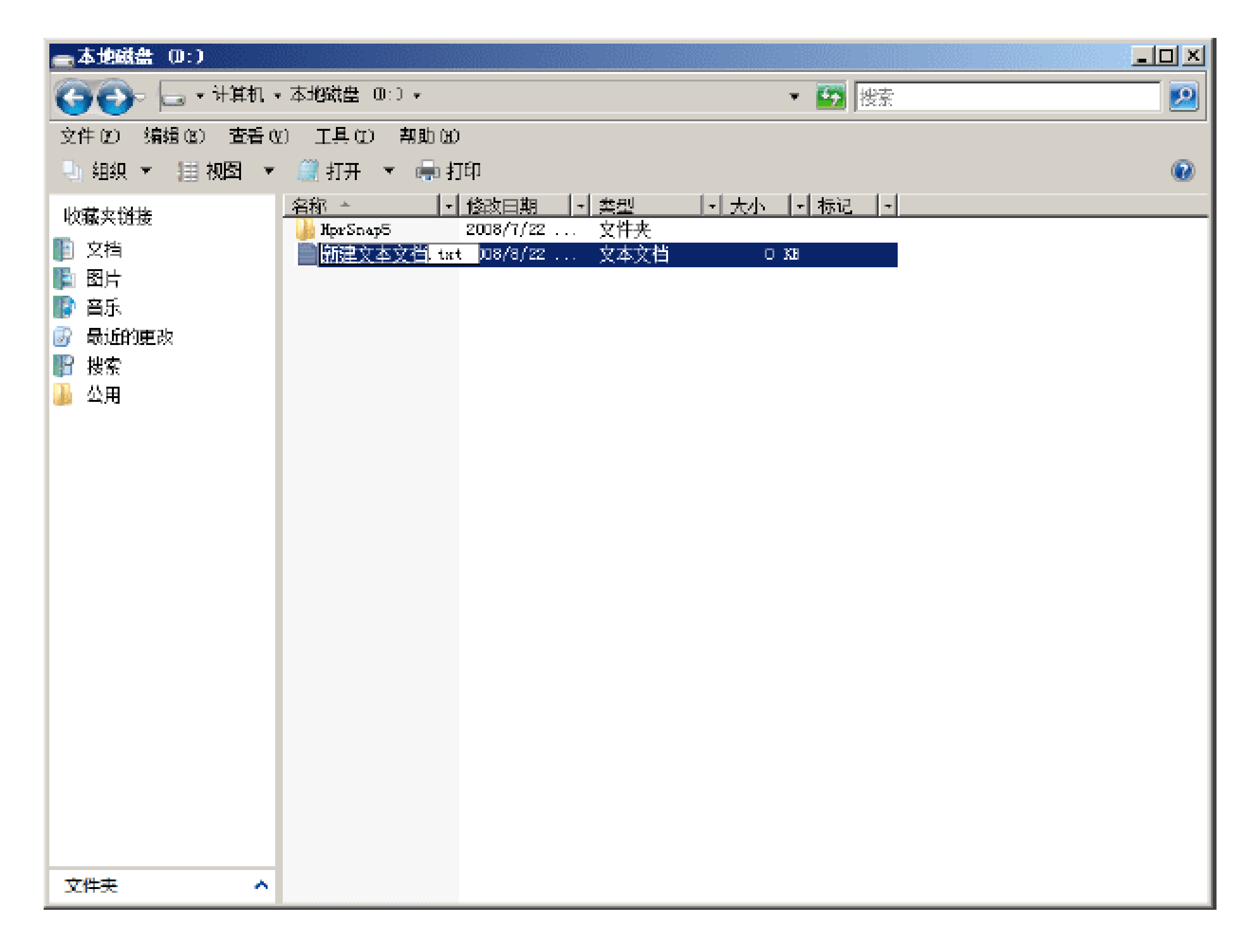


图 6-32 创建测试文本文件

6.1.5 文件权限审核

审核功能可以跟踪用户对指定对象的详细操作，并生成可供管理员查阅的事件日志，提供查看日志中安全事件的方法。这对于监视非法用户入侵以及危及系统数据安全性的尝试是非常必要的。通常情况下，应该被审核的最普通的事件类型包括：

- 访问对象，例如文件和文件夹。
- 用户和组账户的管理员。
- 用户登录以及从系统注销。

1. 审核策略

完成审核之前，必须定制审核策略。审核策略指定了要审核的与安全有关的事件的类别。默认安装 Windows Server 2003/2008 系统时，将关闭所有审核类别。通过打开各种审核事件类别，可以实现符合安全需要的审核策略。如果将对象访问的审核作为审核策略的一部分，则必须打开审核目录服务访问类别(为审核域控制器上的对象)或审核对象访问类别(为审核成员服务器上的对象)。

为将安全威胁的风险降到最低，可以采取多项审核的操作步骤。表 6-3 列出了应该进行审核的各种情况，以及审核事件监视的特定安全危害行为。

表 6-3 审核事件的风险

审核事件	潜在的威胁
登录/注销失败审核	黑客肆意盗取密码
登录/注销成功审核	盗用密码进入
对特权的使用、用户和组管理、安全的更改策略、重新启动、关机和系统事件的成功审核	滥用特权
对文件访问和对象访问事件的成功和失败的审核。文件管理员对可疑的用户或组对敏感性文件的读/写访问进行成功和失败的审核	对敏感性文件的不适当访问

续表

审核事件	潜在的威胁
对文件访问打印机和对象访问事件的成功和失败的审核。打印管理器对那些由可疑用户和组对打印机的访问进行成功和失败的审核	打印机的不适当访问
为程序文件(扩展名为 .EXE 和 .DLL)的写入访问进行的成功和失败审核。成功和失败的审核追踪过程。执行可疑的程序，检查意外修改程序文件或创建意外进程的安全日志。仅在积极监视系统日志时运行	病毒发作

2. 设置审核对象

每个对象都带有一组安全信息或安全描述符。安全描述符部分指定了可以访问对象的组或用户，以及授予这些组或对象的访问类型(权限)。安全描述符中的这一部分称为自由访问控制列表(DACL)。 除了包含权限信息外，对象的安全描述符还包括审核信息。审核信息被称为系统访问控制列表(SACL)。SACL 特别指定了以下操作：

- 访问对象时要审核的组和用户账户。
- 对于每个组或用户需要审核的访问事件。修改文件就是个访问事件的例子。
- 基于对象的 DACL 中授予的每个组或用户的权限的每个访问事件的成功或失败属性。

通常情况下，可被审核的访问类型决定于是否审核对文件和文件夹或 Active Directory 对象的访问。可以对某个对象进行审核，并且通过继承，审核可以应用到任何子对象。例如，如果要审核对文件夹的失败的写入访问，这个审核事件可以被文件夹中所有的文件继承。

3. 设置审核

管理员可以通过设置权限类型将审核策略应用于目标资源上，在安全日志中记录成功访问或失败访问尝试的系统事件，便于管理员更详细地了解用户对目标资源的访问情况。对文件和文件夹访问的审核，首先要求目标资源必须位于 NTFS 分区上，其次必须为对象访问事件设置审核策略。符合以上条件，即可对特定的文件或文件夹进行审核，并且设置对哪些用户或组指定哪些类型的访问事件进行审核。

① 在 Windows 资源管理器中，右击 test 文件夹并选择快捷菜单中的“属性”命令，打开“test 属性”对话框，切换到如图 6-33 所示的“安全”选项卡。

② 单击“高级”按钮，打开“test 的高级安全设置”对话框，切换到“审核”选项卡，显示如图 6-34 所示。在 Windows Server 2008 系统中，默认值是查看当前的审核项目设置情况，而在 Windows Server 2003 系统中，则可以直接更改。

③ 单击“编辑”按钮，显示如图 6-35 所示的对话框，在这里即可修改当前文件夹的审核项目，默认情况下，“审核项目”列表框中空白，即不对任何对象和操作进行审核。

④ 单击“添加”按钮，显示如图 6-36 所示的“选择用户或组”对话框，在“输入要选择的对象名称”文本框中，输入希望被审核的用户账户或组。

⑤ 单击“确定”按钮，显示如图 6-37 所示的对话框，配置希望审核的用户权限，并选中“成功”或“失败”复选框，也可同时选择两者，主要用于设置系统审核日志的记录条件。例如，选择“读取属性”后的“成功”复选框，则系统将只审核用户账户 hstjl 读取目标资源成功的系统事件，而该读取失败的尝试或其他账户的访问均不会被审核。

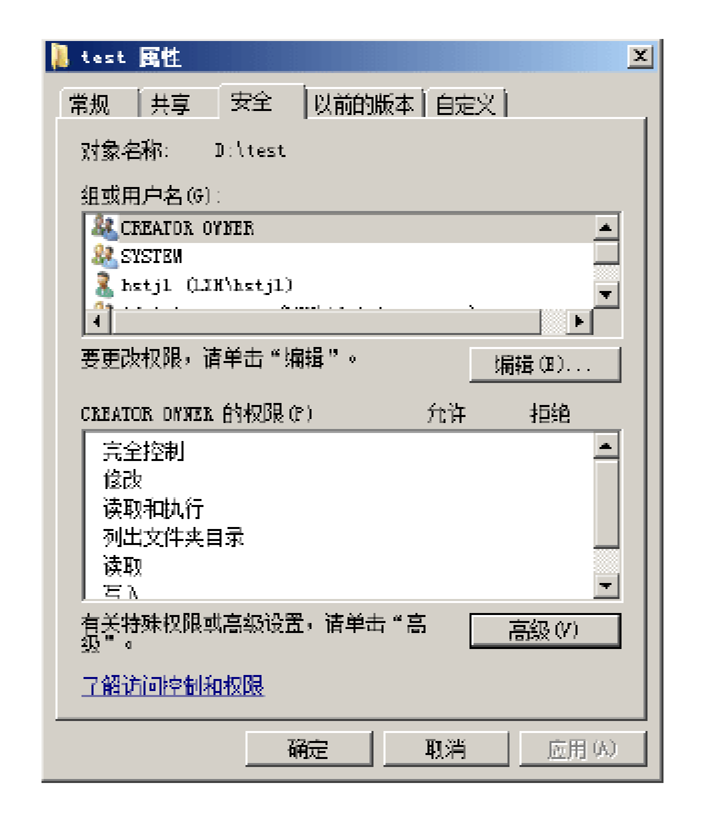


图 6-33　“安全”选项卡

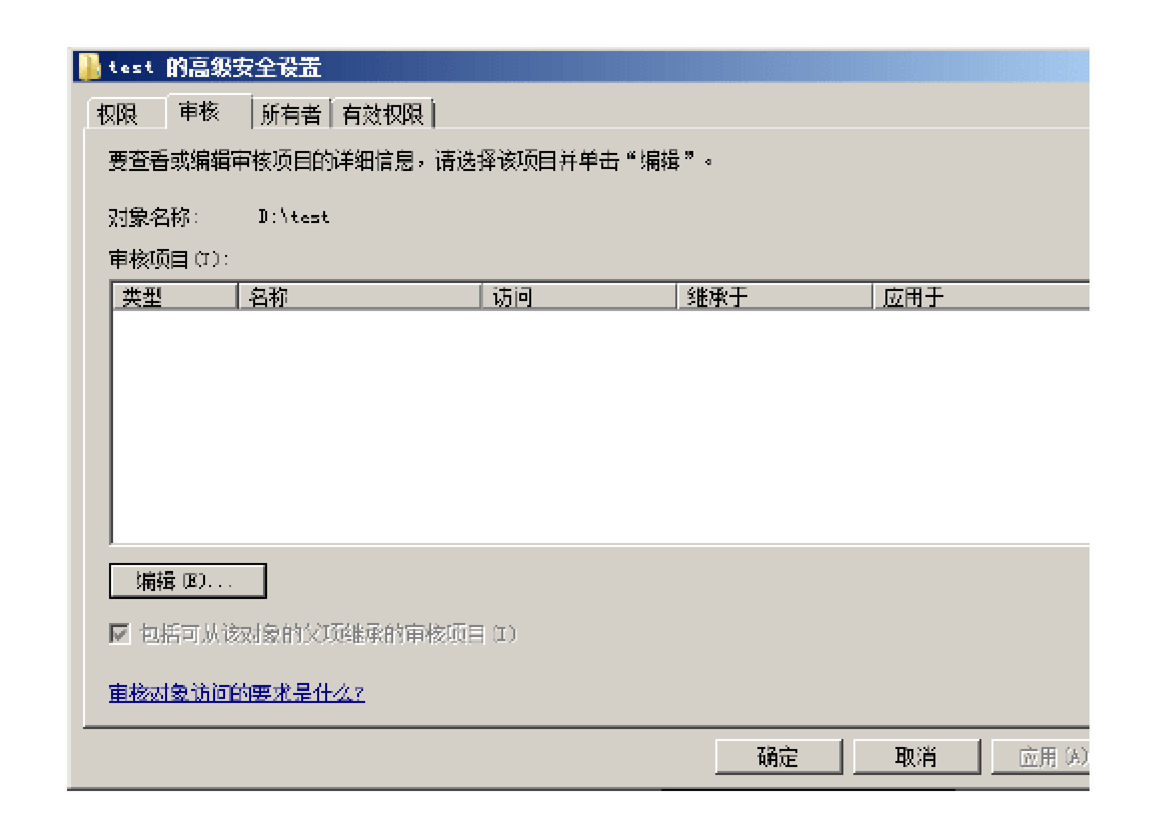


图 6-34　“审核”选项卡

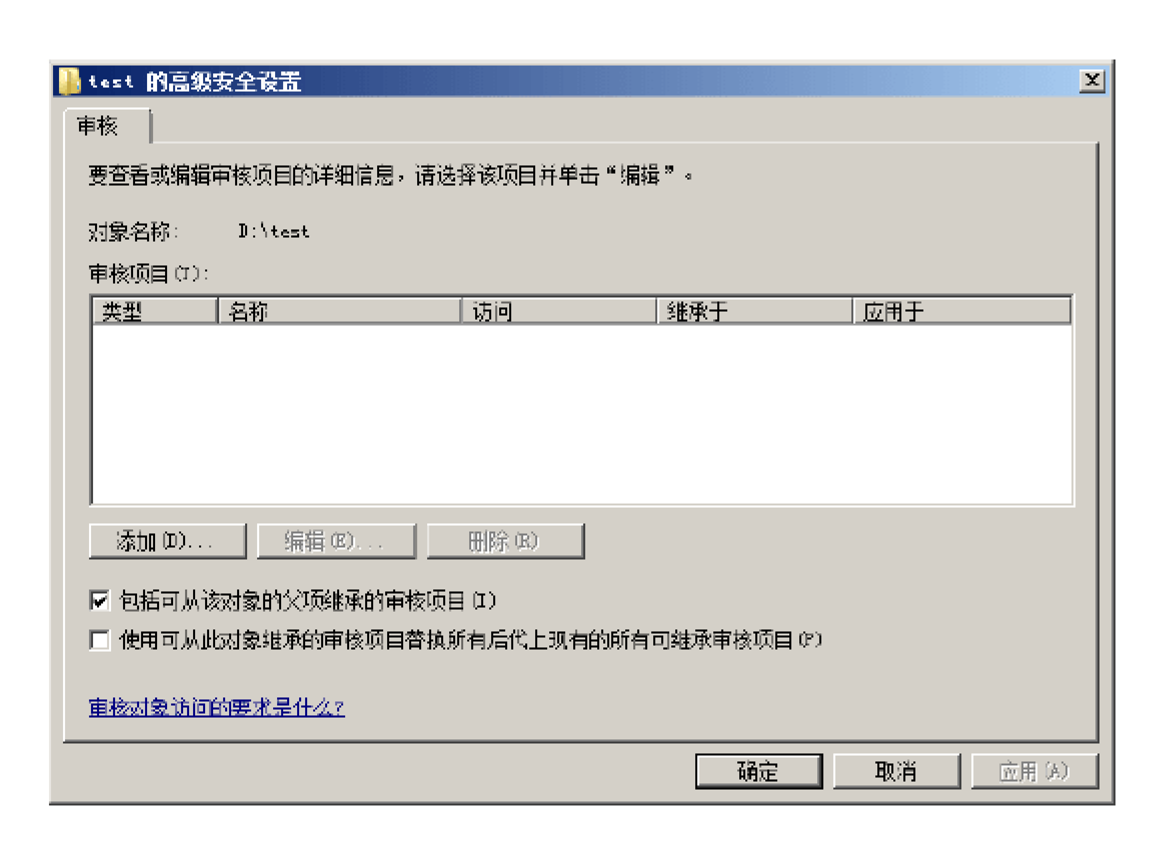


图 6-35　配置审核项目



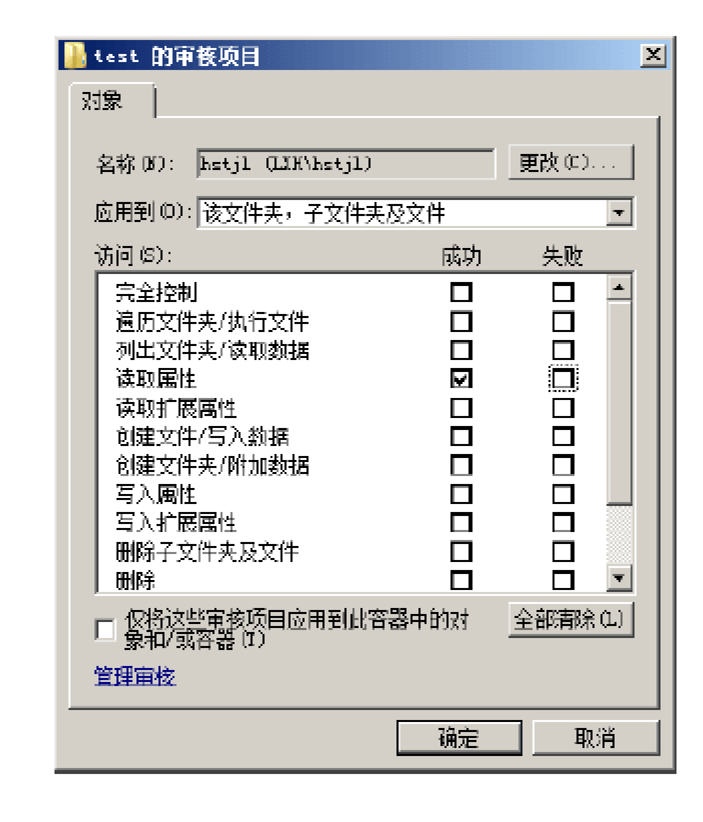


图 6-36　“选择用户或组”对话框　　　　图 6-37　“test 的审核项目”对话框

⑥　连续 4 次单击“确定”按钮保存设置，完成审核设置。重复上述操作，可以设置用于其他账户或操作权限的审核。

6.2　权限管理服务

威胁文件安全的主要因素往往来自内部用户，而普通的访问权限限定很难做到万无一失。Windows Server 2008 系统中的 AD RMS(Rights Management Services，权限管理服务)可以通过数字证书和用户身份验证技术对各种 Office 文档的访问权限加以限制，可以有效防止内部用户通过各种途径擅自泄漏机密文档内容，从而确保了数据文件访问的安全性。

6.2.1　安装 AD RMS 前的准备

相对于先前的 RMS 而言，AD RMS 不再是一个独立服务插件，它已经成为 Windows 的一项内建功能，并且包含了某些升级功能，可以直接在管理服务器窗口中启动安装向导并轻松安装。为了确保安装过程可以顺利进行，开始之前应做好如下准备工作：

- 将计算机加入到域，或者提升为域的额外域控制器，或者子域。
- 使用具有域用户账户登录，但不能使用 Administrator 账户登录。
- 安装 IIS 服务和 ASP.Net 组件。
- 安装 MSMQ(消息队列)服务。
- 选择数据库。如果要使用独立数据库，需安装 SQL Server。否则，可使用 AD RMS 的自带数据库。
- 安装之前，确认 http://uddi.microsoft.com 和 https://uddi.microsoft.com 在 Internet Explorer 中被添加至“受信任的站点”或“本地 Internet”。

6.2.2　安装 AD RMS 服务器

AD RMS 服务并不是 Windows Server 2008 系统默认安装的组件，需要用户手动添加。完成必要的准备工作后，即可开始安装 AD RMS 服务器。另外，用户也可以直接安装 AD RMS 服务器，如果安装向导检测到未安装的组件，则会提示用户，此时通过选择相关选项即可一并完成准备组件的部署。

① 以具有管理员权限的用户账户登录到目标服务器，在“服务器管理器”窗口中，依次选择“角色”→“添加角色”选项，显示如图 6-38 所示的“选择服务器角色”界面。

② 选中 Active Directory Rights Management Services 复选框，显示如图 6-39 所示的对话框，提示是否添加所需的角色服务和功能。如果在此之前，已经完成各项准备工作，则不会显示该对话框。

③ 单击“添加必需的角色服务”按钮，返回如图 6-40 所示的界面，选中 Active Directory Rights Management Services 复选框。



提示：不能使用 Administrator 用户账户登录，否则就会显示如图 6-41 所示的警告框，提示无法安装。

④ 单击“下一步”按钮，显示如图 6-42 所示的 Active Directory Rights Management Services 界面。该界面简要介绍了 Active Directory 权限管理服务的作用以及功能。



图 6-38 “选择服务器角色”界面



图 6-39 添加所需的角色服务和功能



图 6-40 “选择服务器角色”界面



图 6-41 提示更改登录账户



图 6-42 Active Directory Rights Management Services 界面

⑤ 单击“下一步”按钮，显示如图 6-43 所示的“选择角色服务”界面。如果选中“联合身份验证支持”复选框，将同时安装 AD FS 或与当前域中已有的 AD FS 关联使用，它允许用户使用当前域和其他域之间经过联合身份验证的信任关系来建立用户标识，以及提供对其他组织创建的受保护信息的访问权限。不需要联合身份验证的用户建议不要选中该复选框。

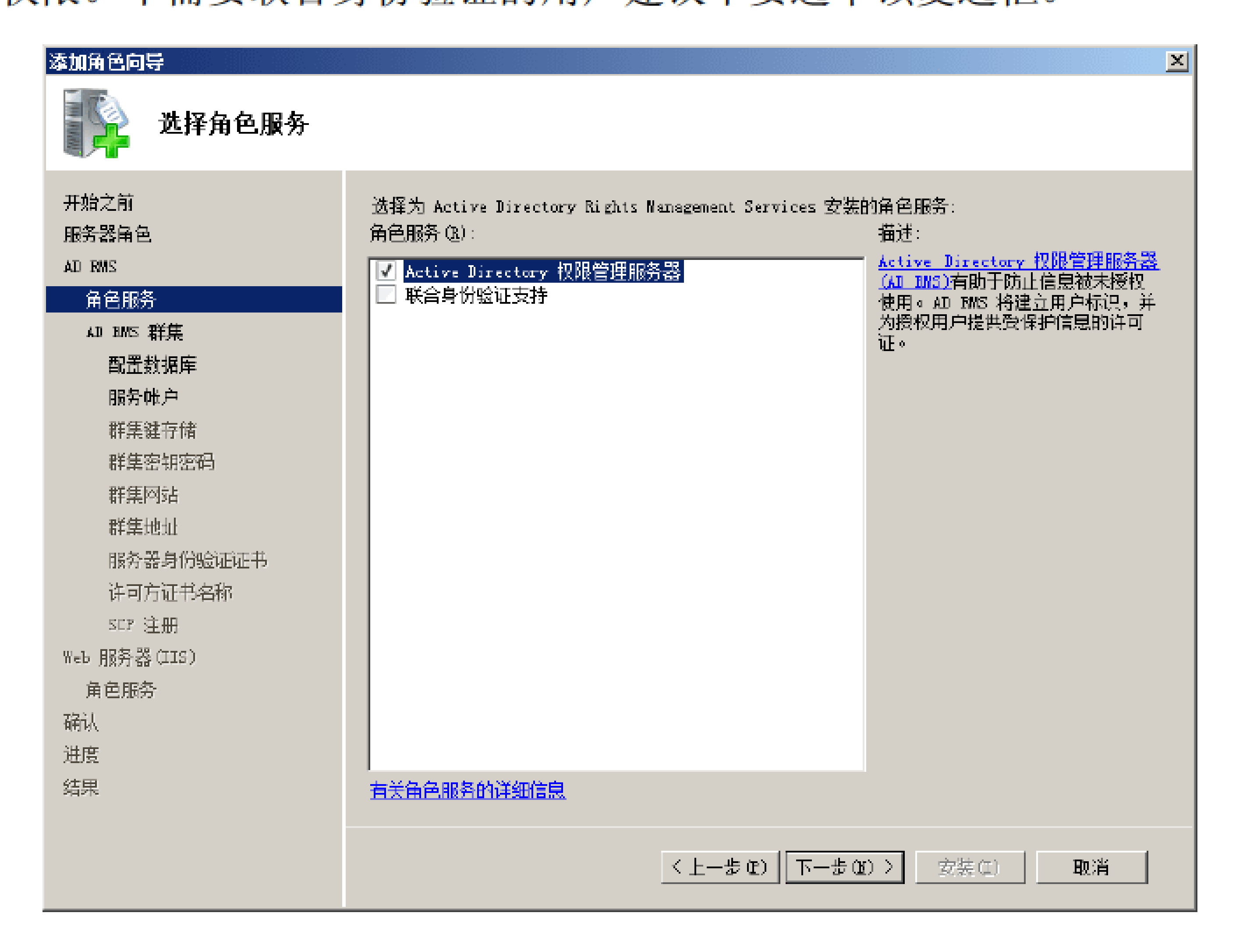


图 6-43　“选择角色服务”界面

⑥ 单击“下一步”按钮，显示如图 6-44 所示的“创建或加入 AD RMS 群集”界面。系统默认选择“新建 AD RMS 群集”单选按钮，由于当前域中没有其他 AD RMS 群集可供加入，所以“加入现有 AD RMS 群集”单选按钮为灰色。安装完成后创建的第一台 AD RMS 服务器即为根群集，后来加入的 AD RMS 服务器为叶服务器。

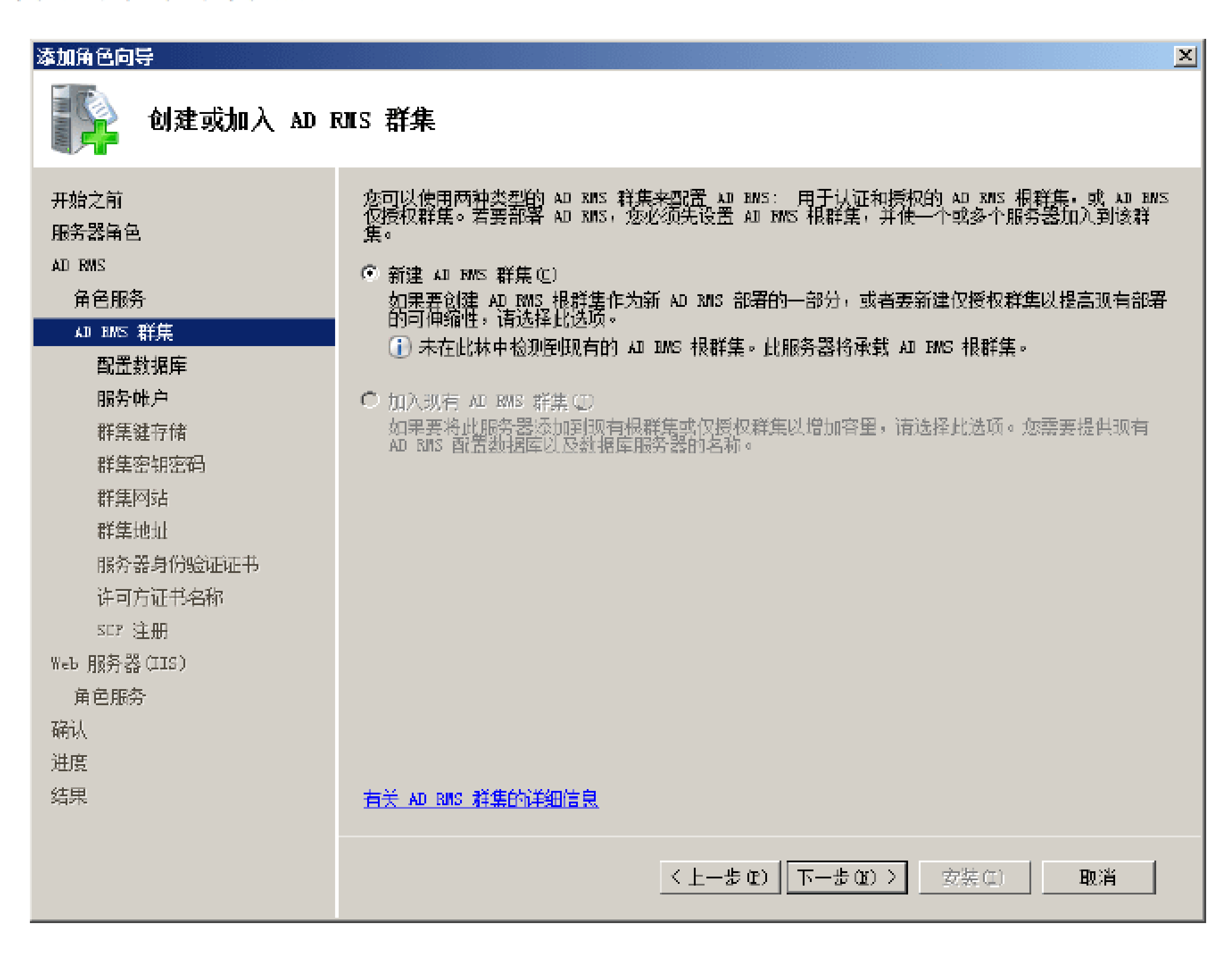


图 6-44　“创建或加入 AD RMS 群集”界面

⑦ 单击“下一步”按钮，显示如图 6-45 所示的“选择配置数据库”界面。如果网络中安装有 SQL Server

服务器，可选择“使用其他数据库服务器”单选按钮；如果要使用 AD RMS 自带的数据库，选择“在此服务器上使用 Windows 内部数据库”单选按钮即可。



图 6-45 “选择配置数据库”界面

注意：选择支持 AD RMS 群集的专用数据库时应注意记录其数据库实例，其他 AD RMS 服务器加入群集时也必须指定相同的实例名称。

⑧ 单击“下一步”按钮，显示如图 6-46 所示的“指定服务账户”界面。该服务账户也就是将来要在 AD RMS 群集中使用的账户，可使用普通域成员账户，但必须区别于当前服务器登录的域用户账户。单击“指定”按钮，显示“Windows 安全”对话框，输入域用户账户。单击“确定”按钮，域控制器会对提交的用户账户和密码进行验证，如果正确无误则返回“指定服务账户”界面。

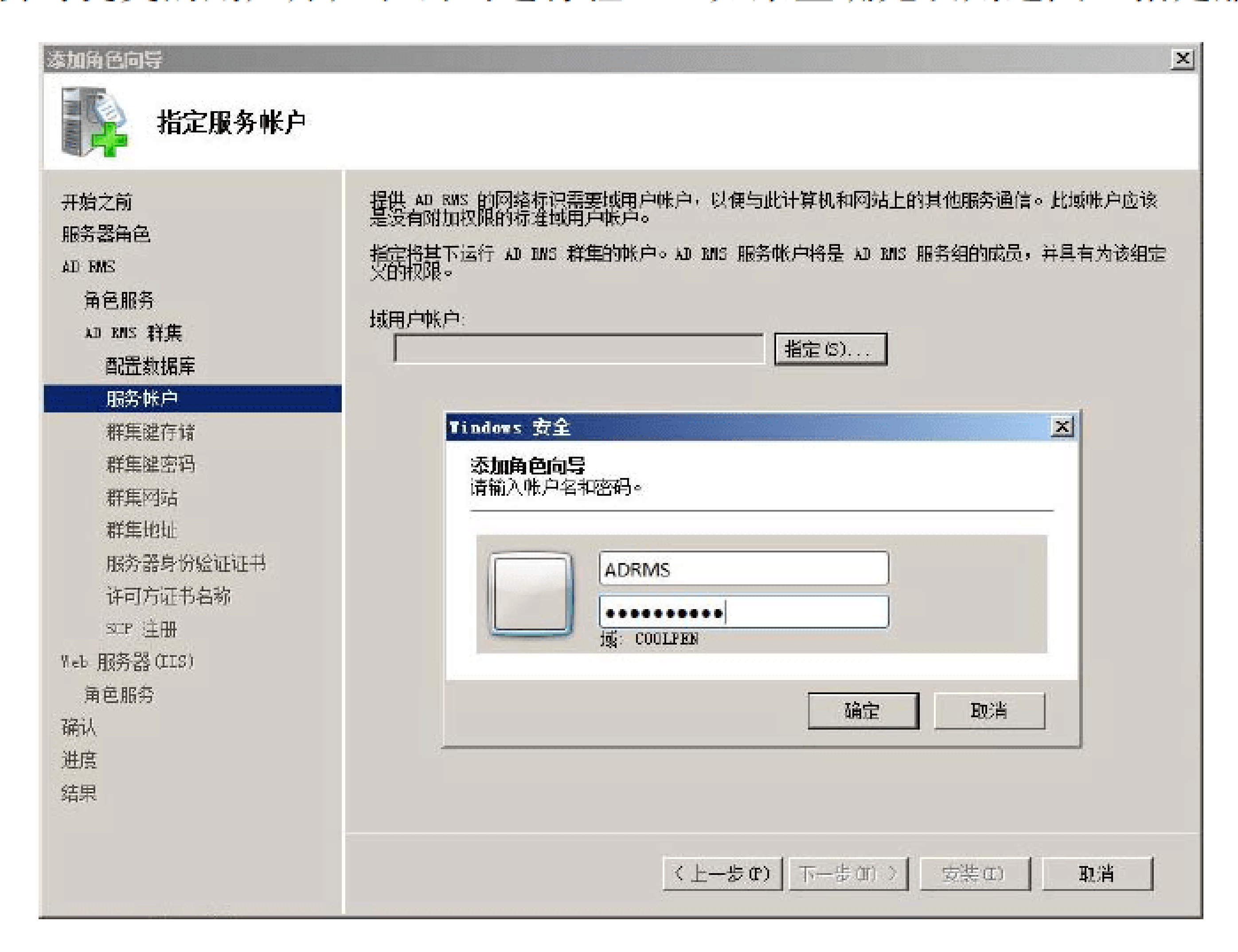


图 6-46 “指定服务账户”界面

⑨ 单击“下一步”按钮，显示如图 6-47 所示的“配置 AD RMS 群集键存储”界面。系统默认选择“使用 AD RMS 集中管理的密钥存储”单选按钮，即由本地服务器自动生成并存储密钥，这里选择该项。该密钥主要用于当前根服务器以及将来叶服务器的灾难恢复，必须牢记。选择“使用 CSP 密钥存储”单选按钮，则需要由专用加密服务器产生并保管该密钥，比较繁琐，但安全性也相对较高。

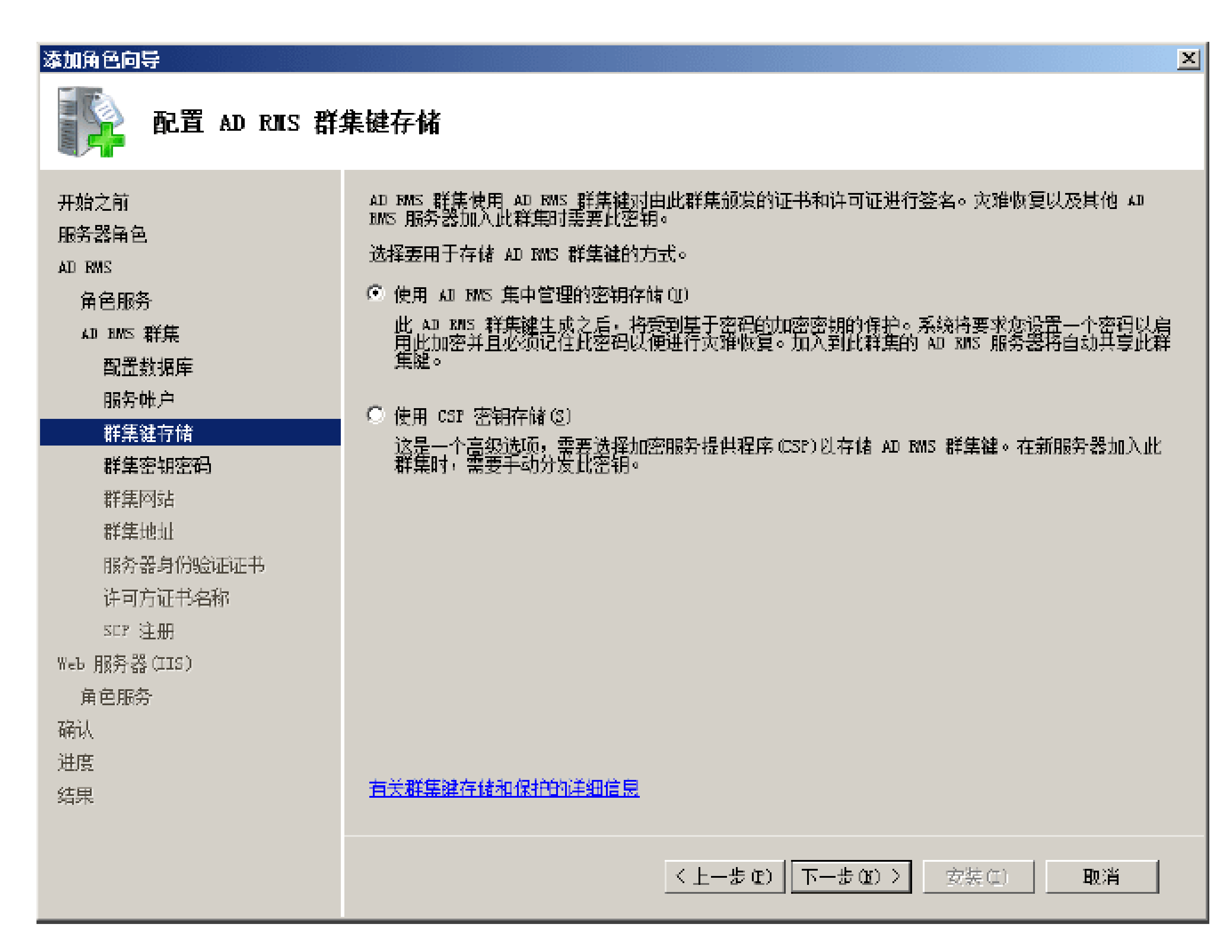


图 6-47　“配置 AD RMS 群集键存储”界面

⑩ 单击“下一步”按钮，显示如图 6-48 所示的“指定 AD RMS 群集密钥密码”界面，其他 AD RMS 服务器加入群集时也要使用此密码，必须妥善保存。

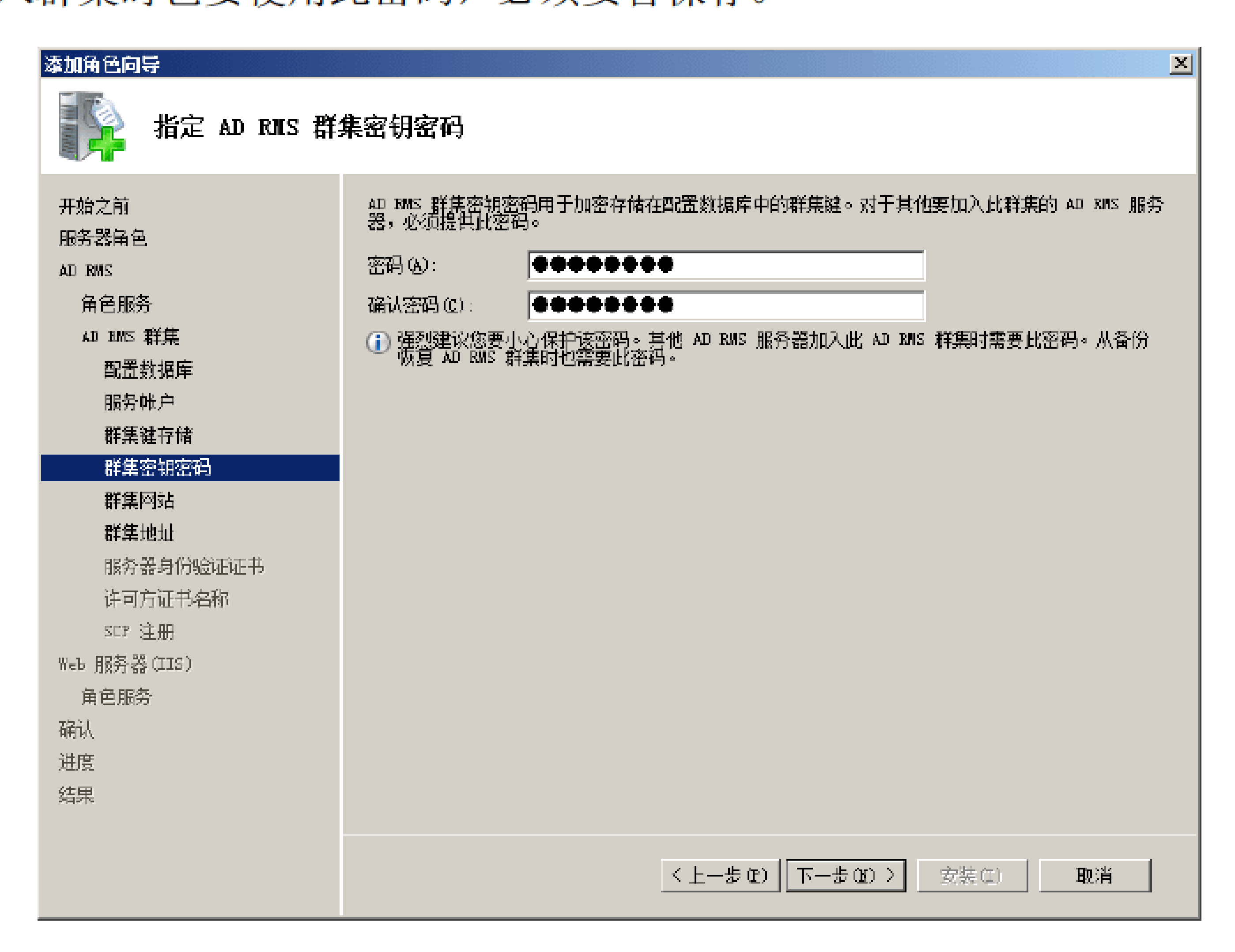


图 6-48　“指定 AD RMS 群集密钥密码”界面

⑪ 单击“下一步”按钮，显示如图 6-49 所示的“选择 AD RMS 群集网站”界面，即管理 AD RMS 群集服务器时使用的站点，准备工作中必须安装 IIS 就是为了在本地创建该站点，保持默认即可。

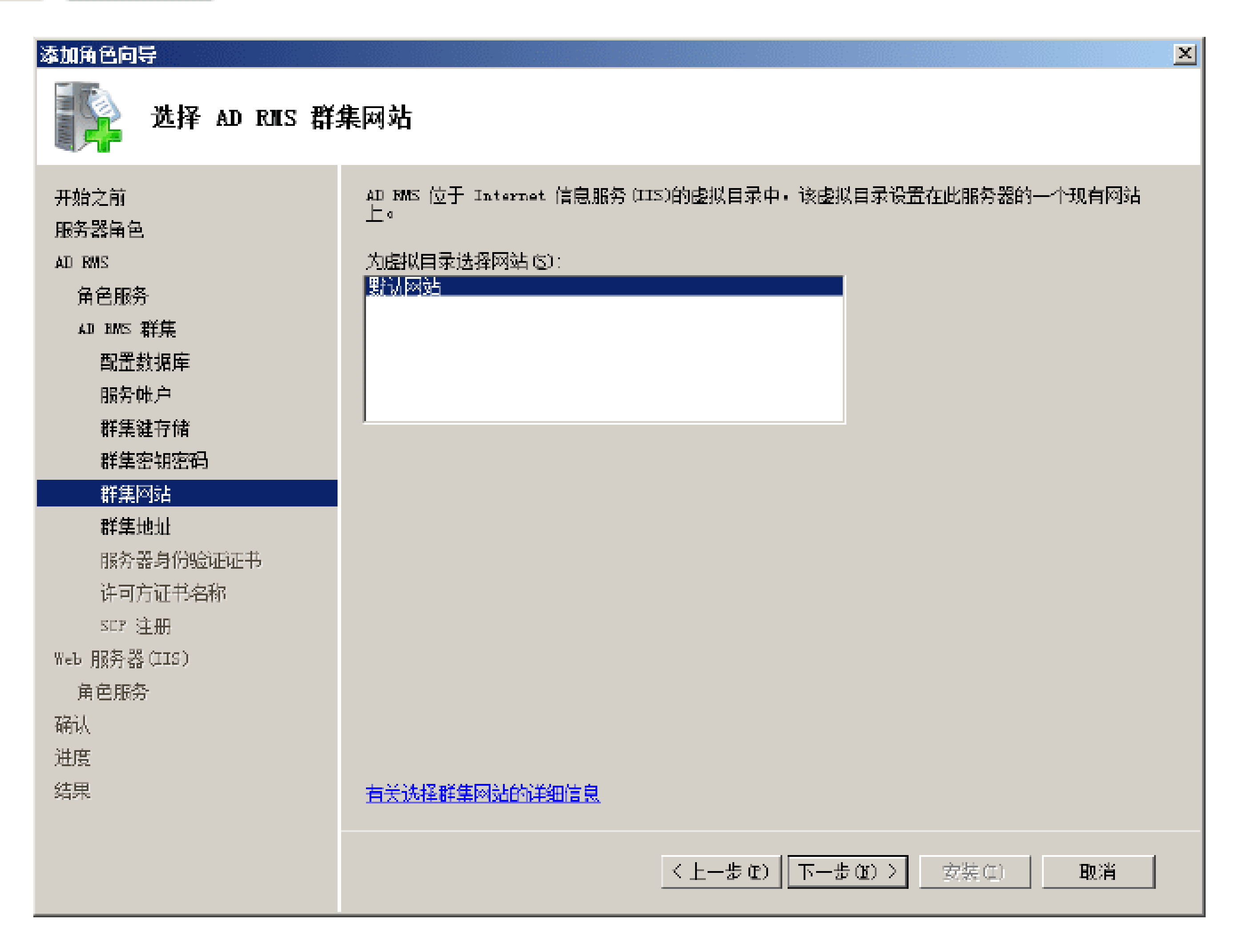


图 6-49 “选择 AD RMS 群集网站”界面

⑫ 单击“下一步”按钮，显示如图 6-50 所示的“指定群集地址”界面。群集地址可以使 AD RMS 客户端通过网络与群集通信。选择“使用 SSL 加密的连接”单选按钮，将使用 SSL 加密，客户端只有得到并安装服务器颁发的数字证书后才能建立连接。在“完全限定的域名”文本框中输入想要使用的域名，如 https://adrms:443 等。SSL 加密连接使用的默认传输端口是 443，客户端访问时也必须使用完整域名。选择“使用未加密的连接”单选按钮，则使用普通传输方式，输入域名，并单击“验证”按钮，确认不与其他站点冲突。

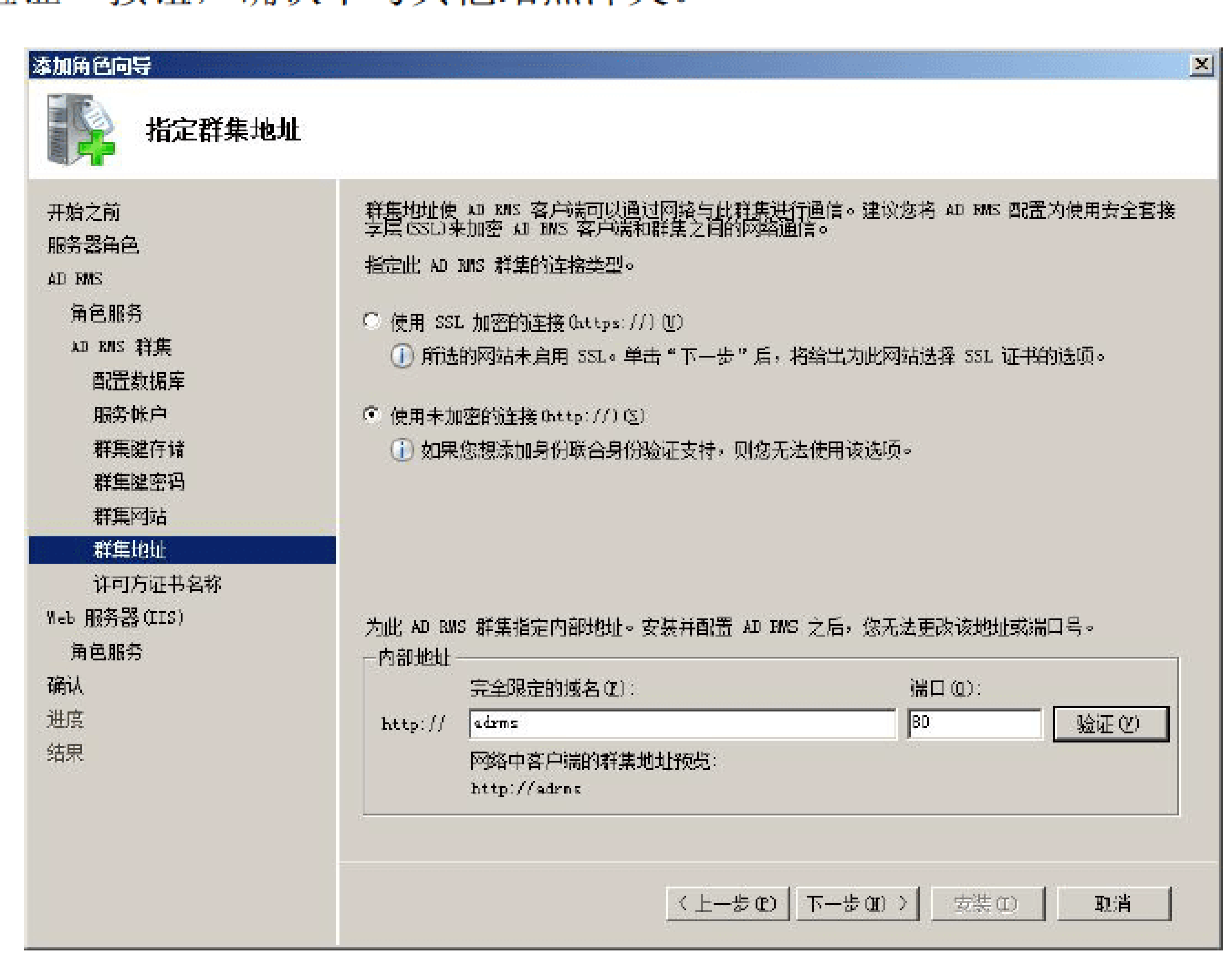


图 6-50 “指定群集地址”界面

注意：自定义端口也可以提升网络连接的安全性，不过，客户端访问时也必须使用相同的端口。



提示：如果选择“使用 SSL 加密的连接”单选按钮，则还需要选择希望用于 SSL 加密的数字证书，可以来自网络中的 CA，也可以使用自签名证书，这里不做详细介绍。

⑬　单击“下一步”按钮，显示如图 6-51 所示的“命名服务器许可方证书”界面，系统默认会以计算机名命名证书，保持默认即可。



图 6-51　“命名服务器许可方证书”界面

⑭　单击“下一步”按钮，显示如图 6-52 所示的“注册 AD RMS 服务连接点”界面。选择“立即注册 AD RMS 服务连接点”单选按钮，在安装完成后立即开始使用此 AD RMS 群集。

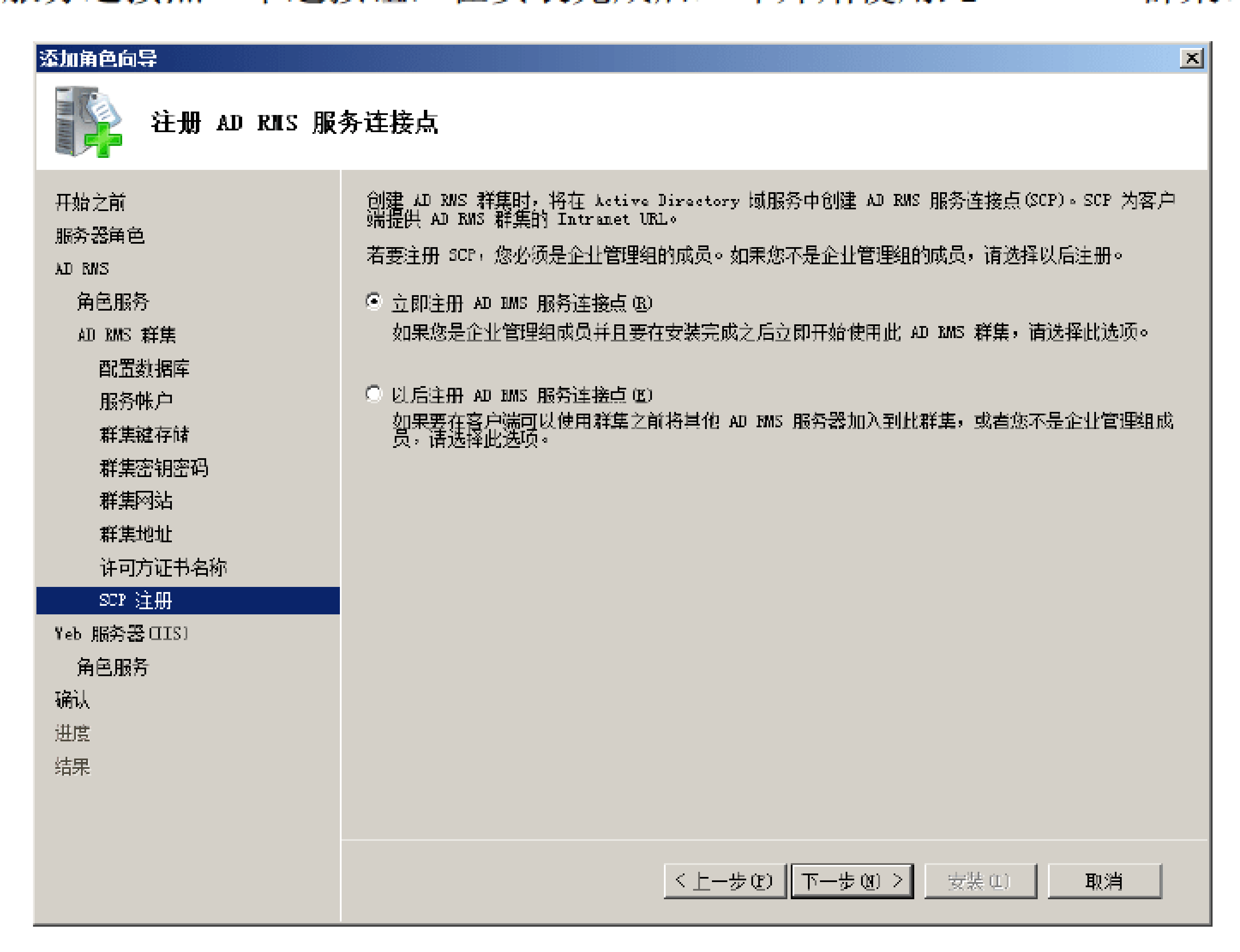


图 6-52　“注册 AD RMS 服务连接点”界面

⑮　单击“下一步”按钮，将显示 IIS 的安装对话框。这里不再赘述。在“确认安装选择”界面中，

显示了要安装的组件信息，如图 6-53 所示。

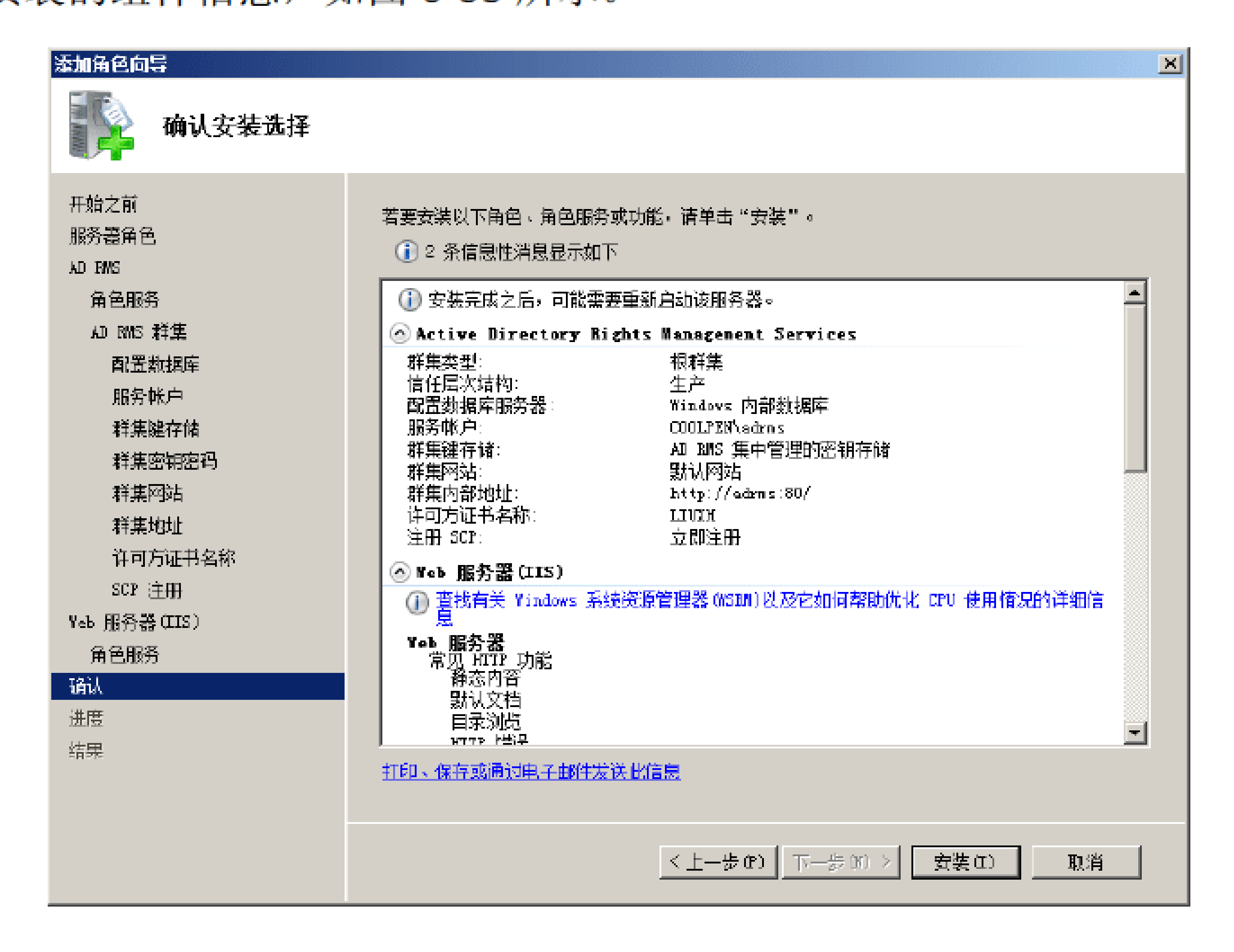


图 6-53　“确认安装选择”界面

⑯　单击“安装”按钮即可开始安装。安装完成后显示如图 6-54 所示的“安装结果”界面，提示安装成功。



图 6-54　“安装结果”对话框

⑰　单击“关闭”按钮，退出安装向导。根据提示信息，注销当前系统并重新登录。

6.2.3　配置 AD RMS 服务器

AD RMS 采用 MMC 控制台管理的方式，提供权限管理服务之前必须进行简单配置，如创建信任策略、权限模板等。依次选择“开始”→“管理工具”→Active Directory Rights Management Services 选项，启动 AD RMS 控制台，如图 6-55 所示。如果选择 SSL 加密连接的方式，则在此过程中可能会出现“安全警报”

提示框，直接单击“是”按钮跳过即可。

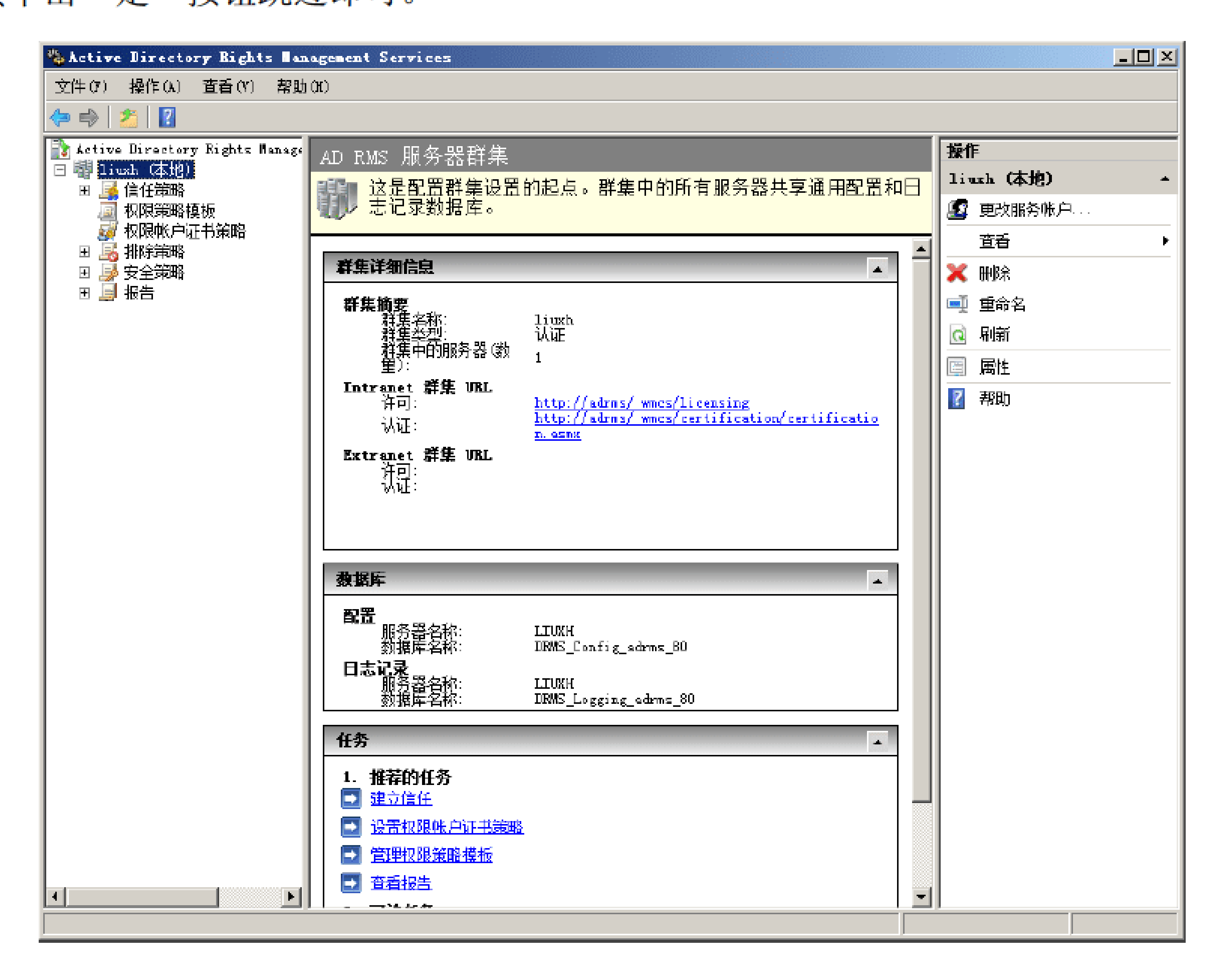


图 6-55　AD RMS 控制台

1. 配置信任策略

信任策略是不同 AD RMS 群集或不同域林中的 AD RMS 服务器之间建立信任关系的唯一标准，主要包括“受信任的用户域”和“受信任的发布域”。

(1) 受信任的用户域

默认情况下，只有受信任的用户域才可以使用当前 AD RMS 服务器提供的权限保护服务，不同 AD RMS 群集或不同林中的 RMS 服务器都是通过彼此的许可证书识别的。用户可以通过将其他 AD RMS 群集中的信任用户域导出，并添加至本地服务器中，来实现对其他用户提供权限管理服务。导出的信任用户域文件中会包括原 AD RMS 服务器的许可证信息，因此建立信任关系后，来自该域的用户就可以使用当前 AD RMS 服务器提供的使用许可证。

① 在 AD RMS 控制台窗口中，依次选择“信任策略”→“受信任的用户域”选项，显示如图 6-56 所示的“受信任的用户域”窗格。在“受信任的用户域信息”列表框中默认显示的是本地用户域，右击并选择快捷菜单中的“属性”命令即可查看其详细信息。

② 在右侧的“操作”栏中，单击“导入受信任的用户域”链接，显示如图 6-57 所示的“导入受信任的用户域”对话框，在“受信任的用户域文件”文本框中输入文件的保存路径，或单击“浏览”按钮选择，在“显示名称”文本框中，输入该用户将在列表中显示的名称，用来进行标识。

③ 单击“完成”按钮，即可完成用于域的添加。重复操作，可添加多个受信任的用户域。



提示： 在“受信任的用户域信息”列表框中，右击域并选择快捷菜单中的“导出受信任的用户域”命令，还可以将其导出，以备本地恢复使用，也可以导入到其他 AD RMS 群集中，用于接受其他 AD RMS 服务器的权限许可证。

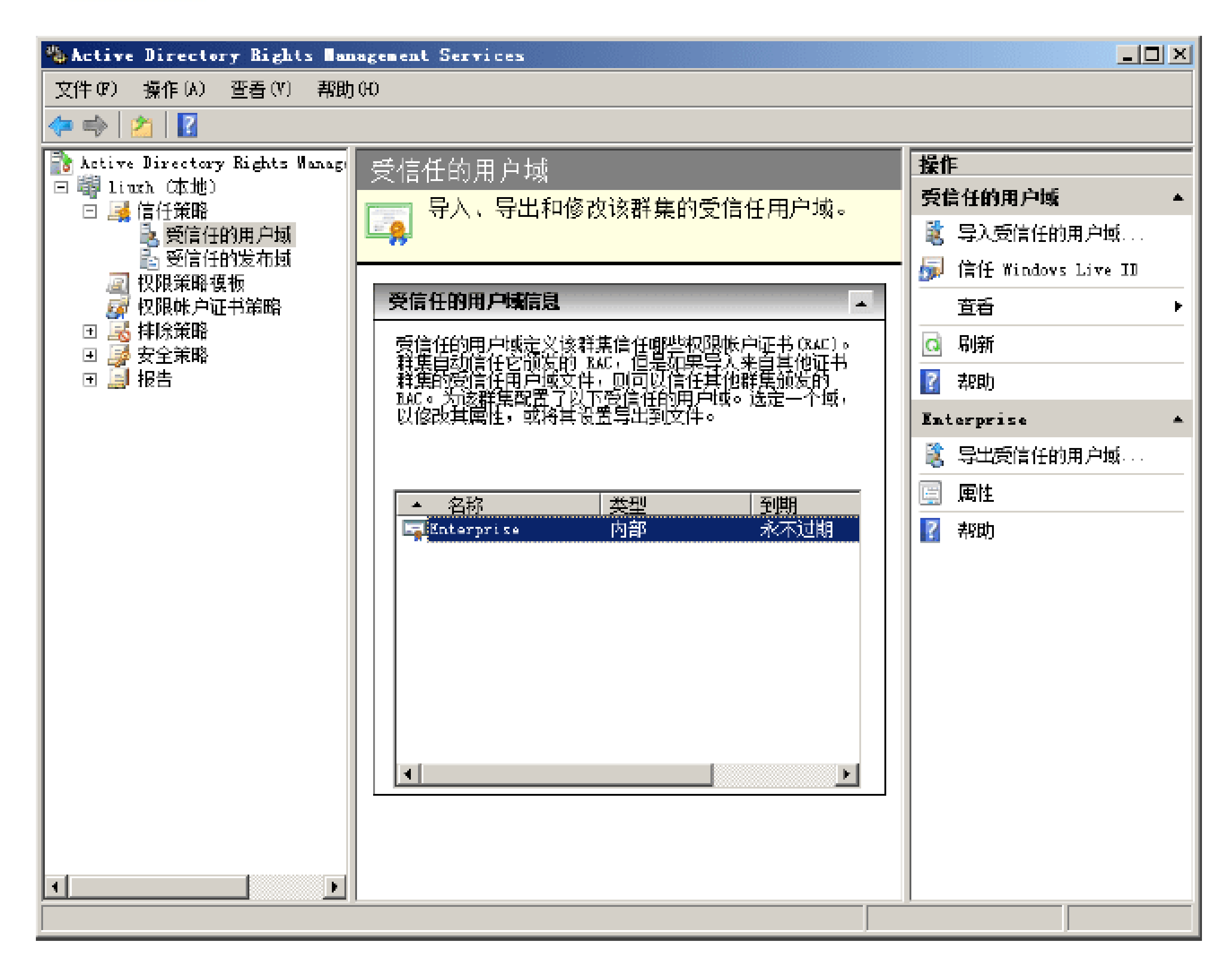


图 6-56　受信任的域用户



图 6-57　导入受信任的用户域

(2)　受信任的发布域

在 AD RMS 控制台窗口中，单击“受信任的发布域”显示如图 6-58 所示的“受信任的发布域信息”窗口。

受信任的发布域用于定义哪些 AD RMS 群集发布的许可证受到此群集的信任，与受信任的用户域恰恰相反，列表中默认存在的是本地服务器的记录。受信任的发布域文件的导出和导入与受信任的用户域文件类似，不同的是发布域文件的类型为.XML，其中包括将要信任的 AD RMS 服务器许可方证书、群集密钥和模板等信息。另外，发布域文件本身是受密码保护的，导入时必须输入原 AD RMS 服务器上使用的存储密码。

2. 配置权限策略模板

(1)　创建权限策略模板

机密程度不同的文档发布到客户端后设置的权限也有所不同，此时就需要为该文档应用不同级别权限

的策略模板。权限策略模板是为定义用户的权限策略用的，管理员可以通过定制一些现成的策略模板让企业用户直接调用。

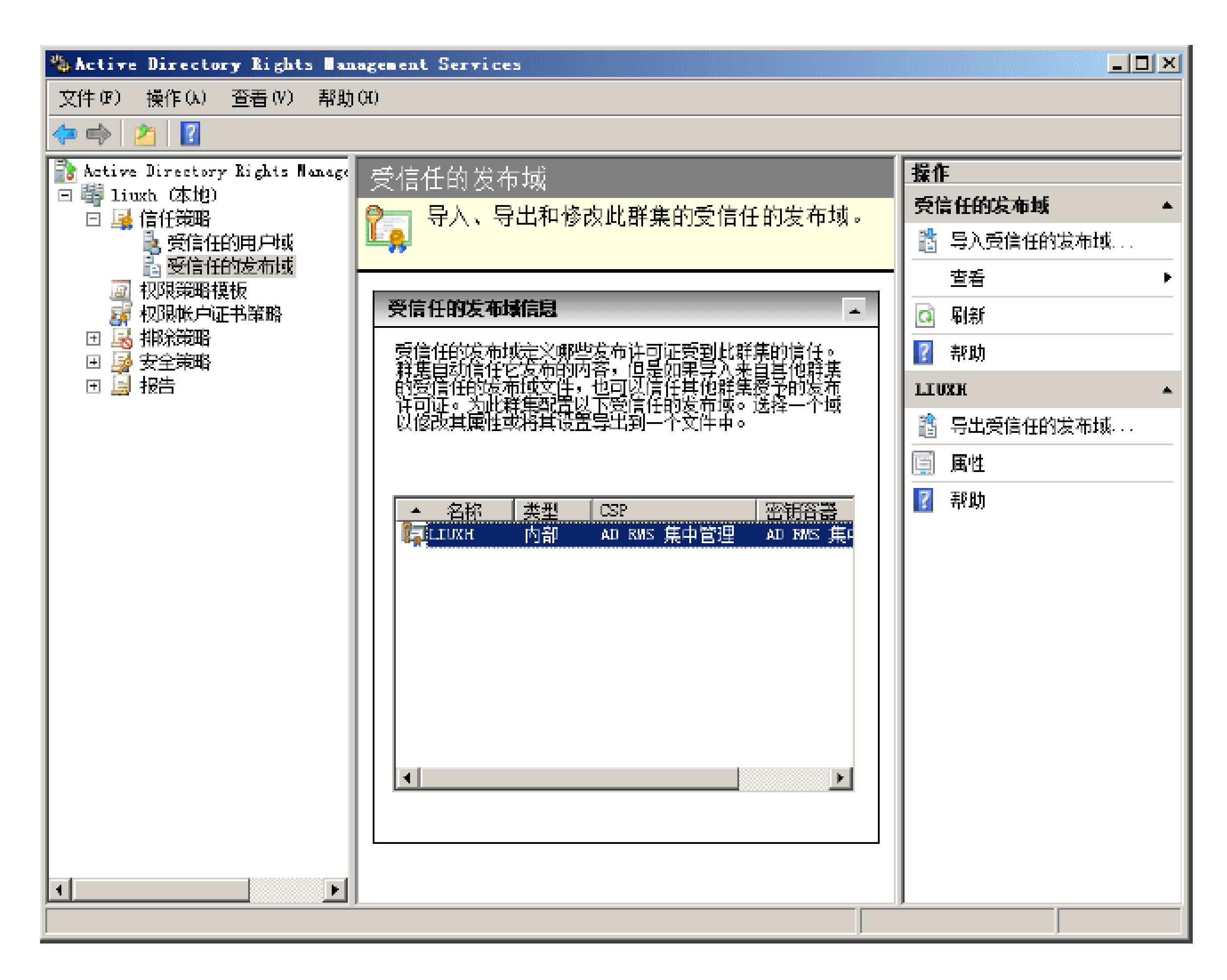


图 6-58　受信任的发布域

① 在“AD RMS 控制台”窗口中，单击“权限策略模板”显示如图 6-59 所示的“分布式权限策略模板”窗格。

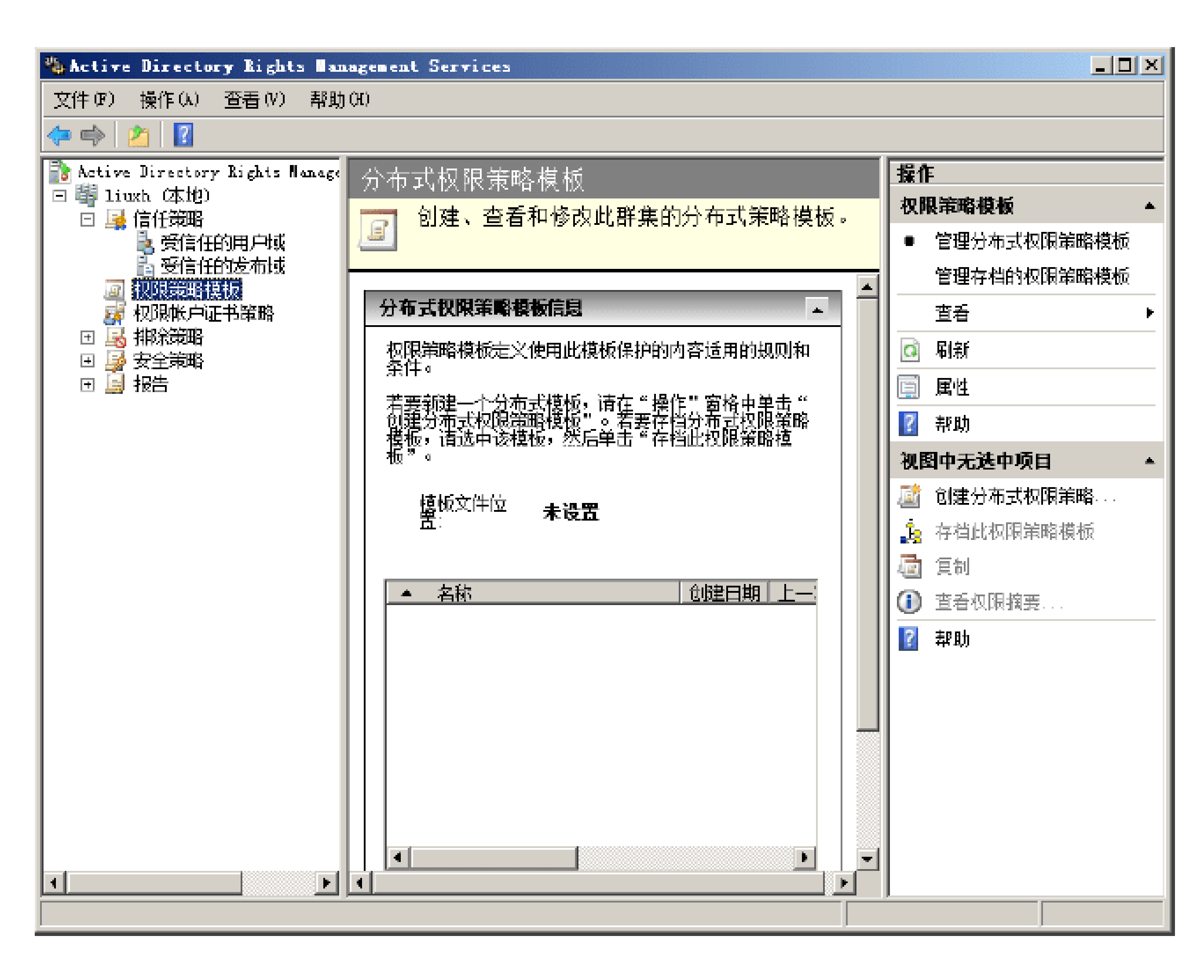
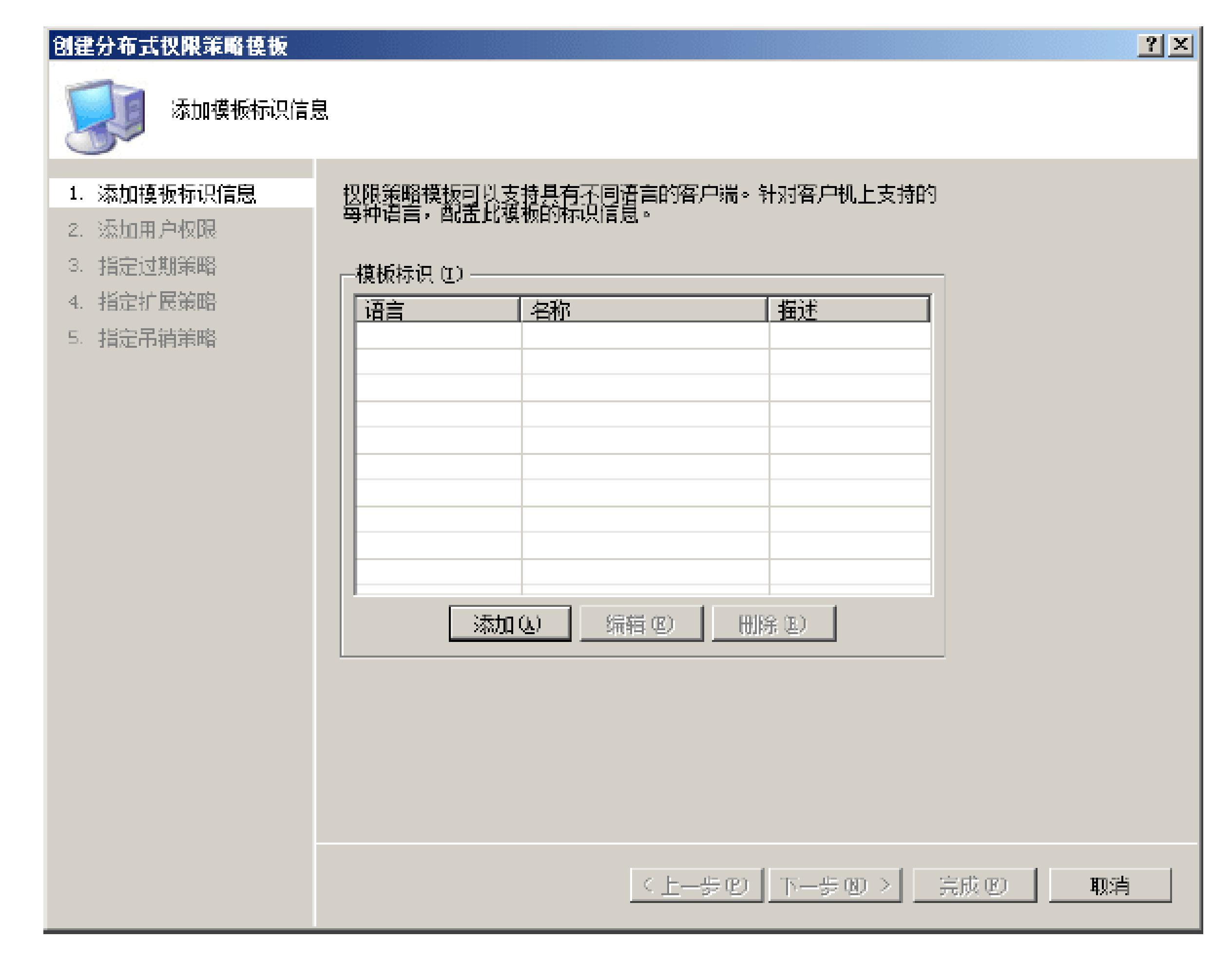


图 6-59　“分布式权限策略模板”窗格

② 单击“操作”栏中的“创建分布式权限策略模板”链接，启动创建向导，首先显示如图 6-60 所示的“添加模板标识信息”界面。

③ 单击“添加”按钮，显示如图 6-61 所示的“添加新的模板标识信息”对话框。在“名称”文本框中输入新建模板的名称，在“描述”列表框中输入相关描述信息。单击“添加”按钮，将其添加

至“模板标识”列表框中。



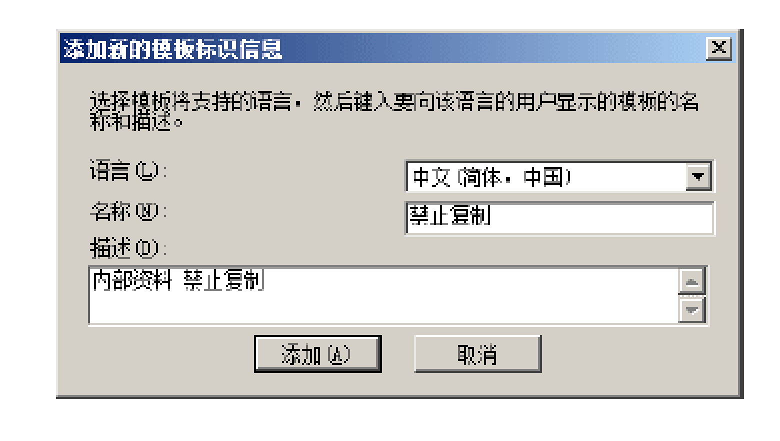



图 6-60 “添加模板标识信息”界面

图 6-61 “添加新的模板标识信息”对话框



提示：“语言”下拉列表框是专为使用不同语言的客户端设置的，如果客户端只支持英文显示，则可以在“添加模板标识信息”界面中再次单击“添加”按钮，并选择“英文”语言即可。需要注意的是，要想使选择的语言生效，必须先在服务器上安装该语言。

④ 单击“下一步”按钮，显示如图 6-62 所示的“添加用户权限”对话框，默认情况下“用户和权限”列表框是空的，即只有“授予所有者不会过期的完全控制权限”，其他用户账户没有任何权限。

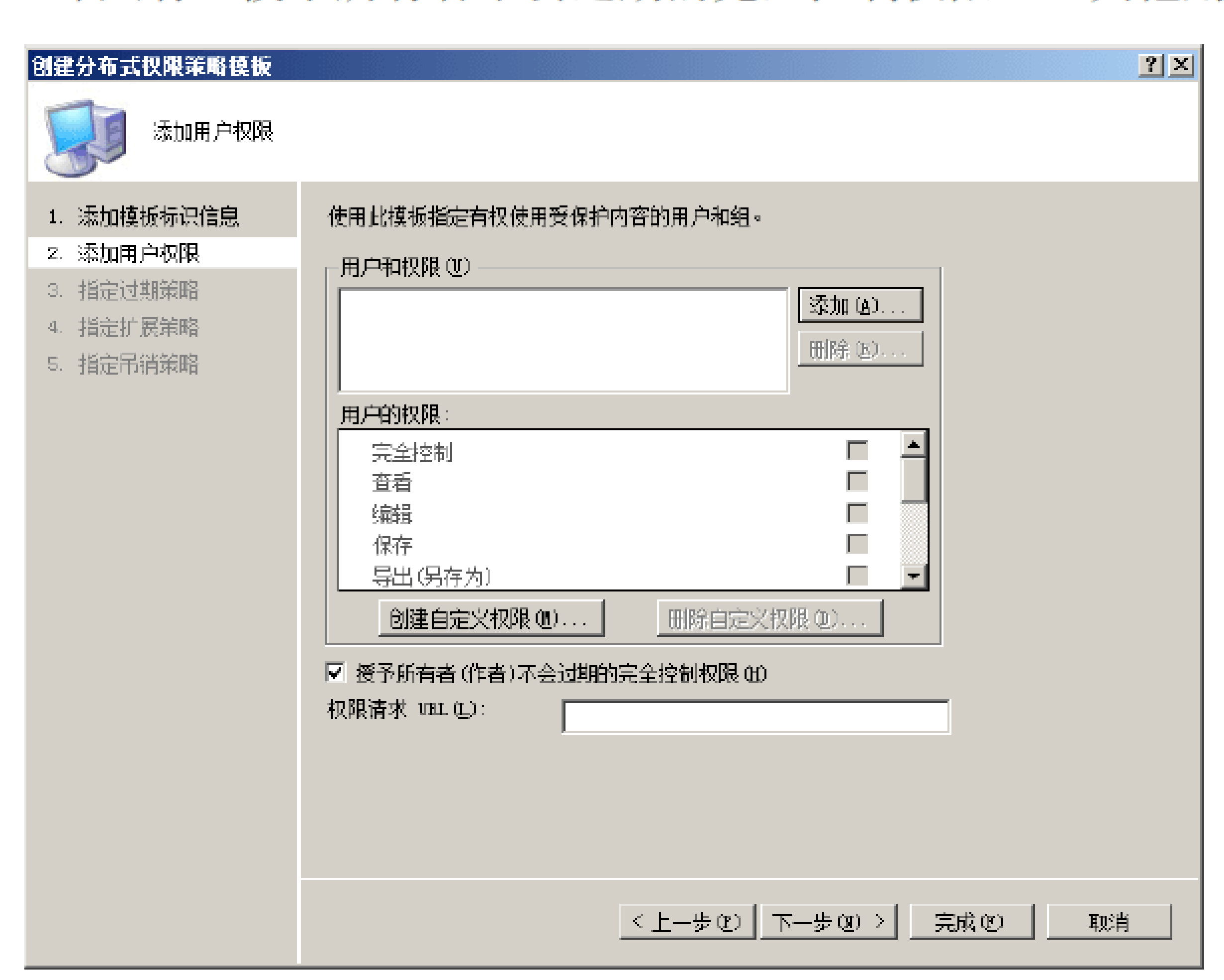


图 6-62 “添加用户权限”界面

⑤ 单击“添加”按钮，显示如图 6-63 所示的“添加用户或组”对话框。选择“用户或组的电子邮件地址”单选按钮，即可在下面的文本框中输入用户对应电子邮件地址，也可以单击“浏览”按钮，打开“选择用户或组”对话框，直接从当前域控制器中查找添加。如果选择“任何人”单选按钮，

则对当前域中的所有用户账户有效。



注意：如果要添加用户，应事先在域控制器上，打开用户属性对话框，为用户添加电子邮件地址，如图 6-64 所示。同样，如果要添加用户组，也要打开用户组属性，添加电子邮件地址。

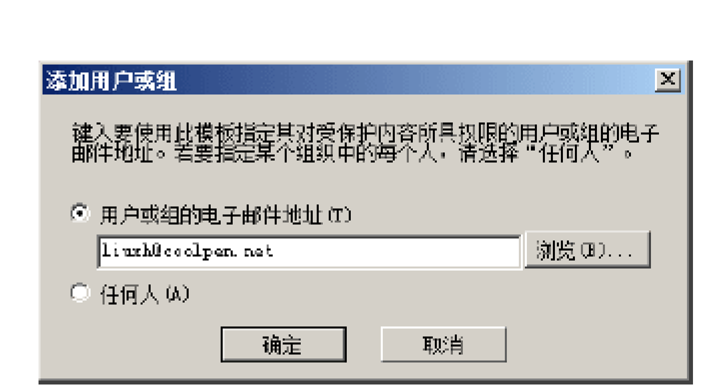


图 6-63　“添加用户或组”对话框

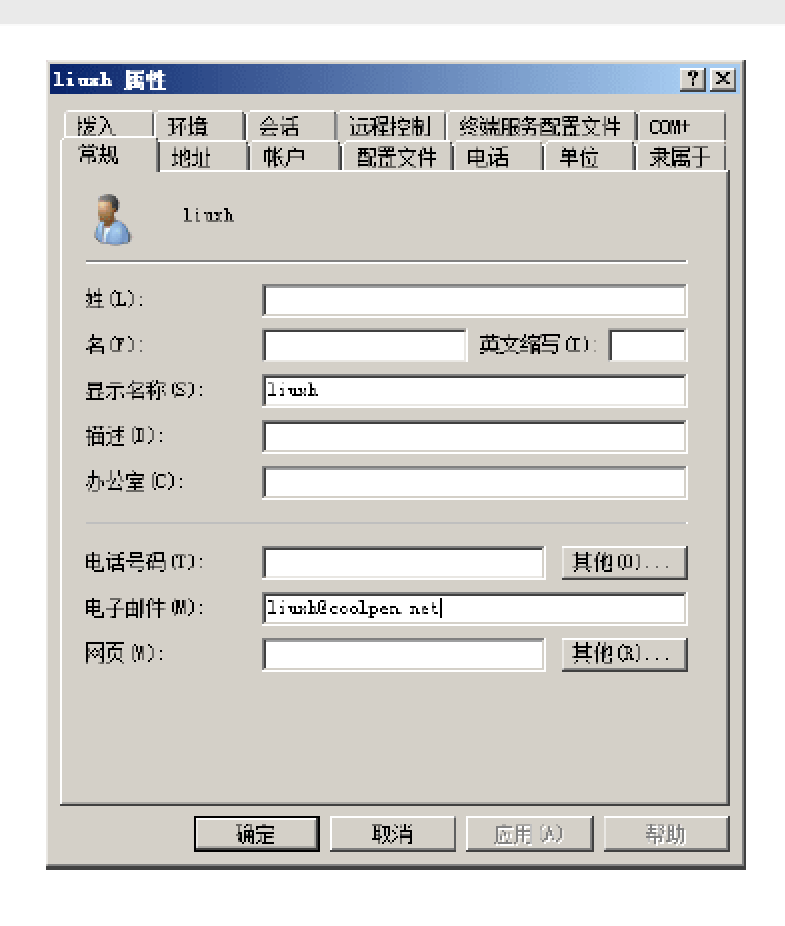


图 6-64　添加用户电子邮件

⑥　单击“确定”按钮，将所选用户添加至列表框中，如图 6-65 所示。重复操作，可添加多个用户或组的电子邮件地址。然后，在“用户和权限”列表框中，选择赋予用户的权限，例如，要求做到“禁止复制”，则只选中“查看”复选框即可。

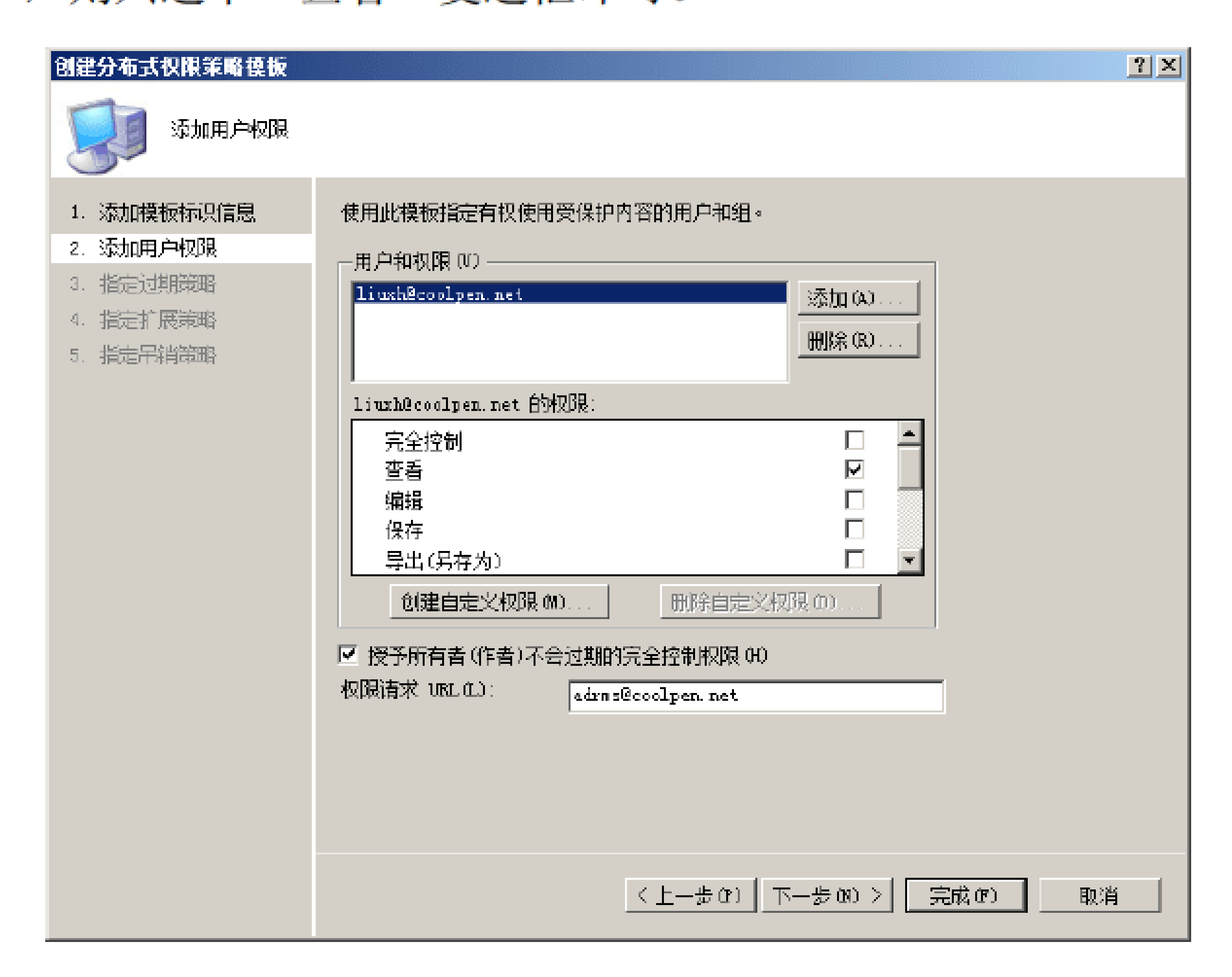
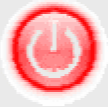


图 6-65　指定用户权限

“权限请求 URL”是当模板赋予用户的权限无法完成相应工作，或在模板权限规定的时间和日期内没有完成工作时，用户可以通过此 URL 继续向管理员发出权限请求，以再次获得权限或附加权限。



注意：权限列表框中给出的所有权限都是允许的，即只要选中某项，就表示要赋予用户具有相应的权限。

⑦ 单击“下一步”按钮，显示如图 6-66 所示的“指定过期策略”界面。在“内容有效期限”选项区域中，可以定义当前模板中的权限信息何时过期或有效期限等，默认为“永不过期”。内容过期后，如果仍需要使用该策略信息，则必须重新发布一次。



图 6-66 “指定过期策略”界面

⑧ 单击“下一步”按钮，显示如图 6-67 所示的“指定扩展策略”界面。

■ “使用户能够使用浏览器加载项查看受保护的内容”：该项对于没有安装 Office 的客户端是非常实用的，只需安装相关插件即可在浏览器中查看受 RMS 保护的 Office 文档，建议选择该项。

■ “每次使用内容时需要更新使用许可证(禁用客户端缓存)”：该项虽然可以使被保护文档更安全，但客户端每次使用时就会非常繁琐。

■ “如果您要为启用 AD RMS 的应用程序指定其他信息，则可以在此处以名称-值对的形式指定”：选中该复选框，可在下面的列表中添加特定应用程序需要的名称和权限值，普通用户无需设置。

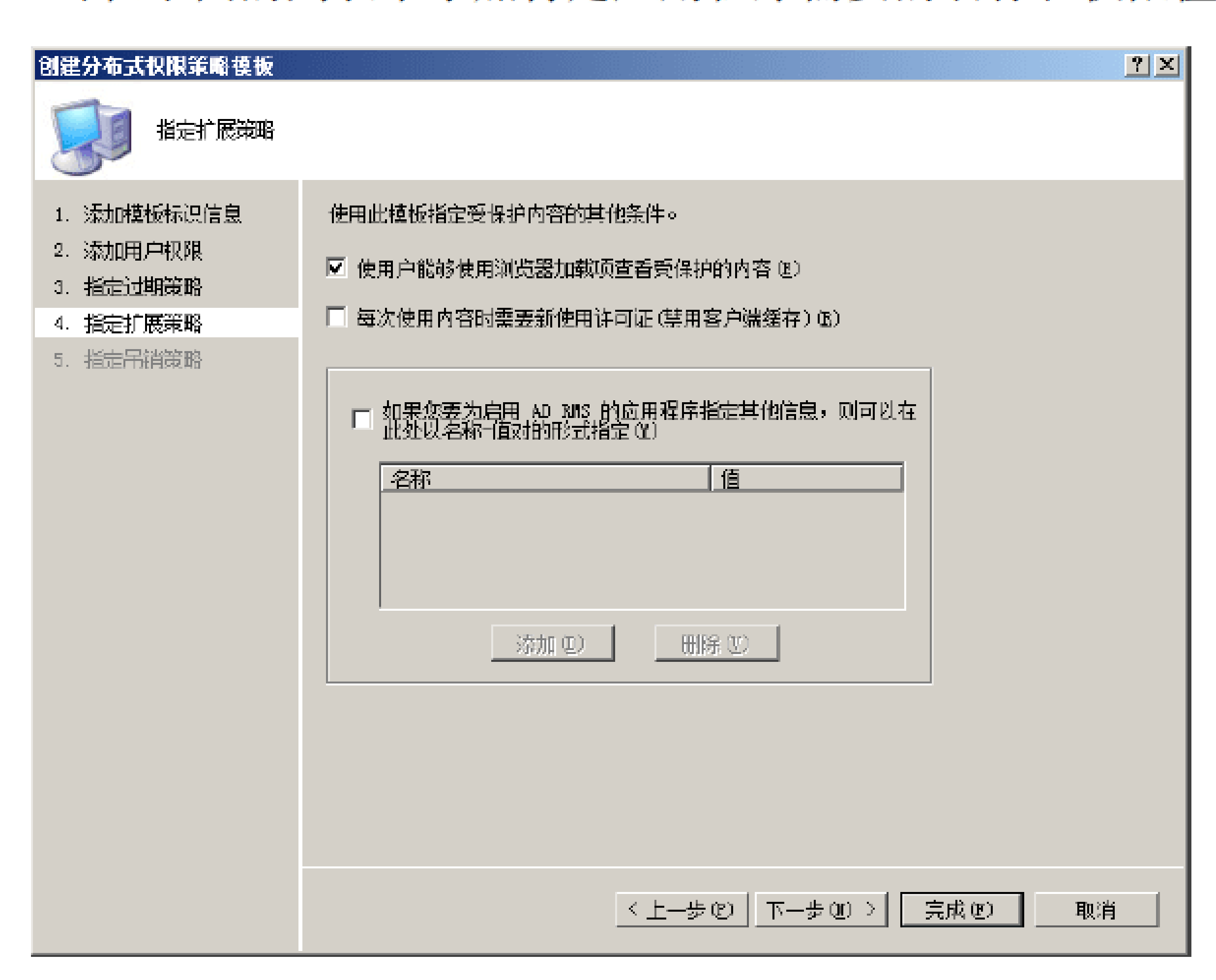


图 6-67 “指定扩展策略”界面

⑨ 单击“下一步”按钮，显示如图 6-68 所示的“指定吊销策略”界面。吊销是 AD RMS 的一项重要

功能，实施吊销之前必须先手动创建一个吊销列表，并为每个吊销列表生成一个公钥/私钥对，然后使用私钥签署吊销列表；另外，还必须为吊销列表指定一个用户可以访问的 URL 地址或 UNC 路径。通常情况下，不需要 AD RMS 服务器吊销，即不选中该复选框。

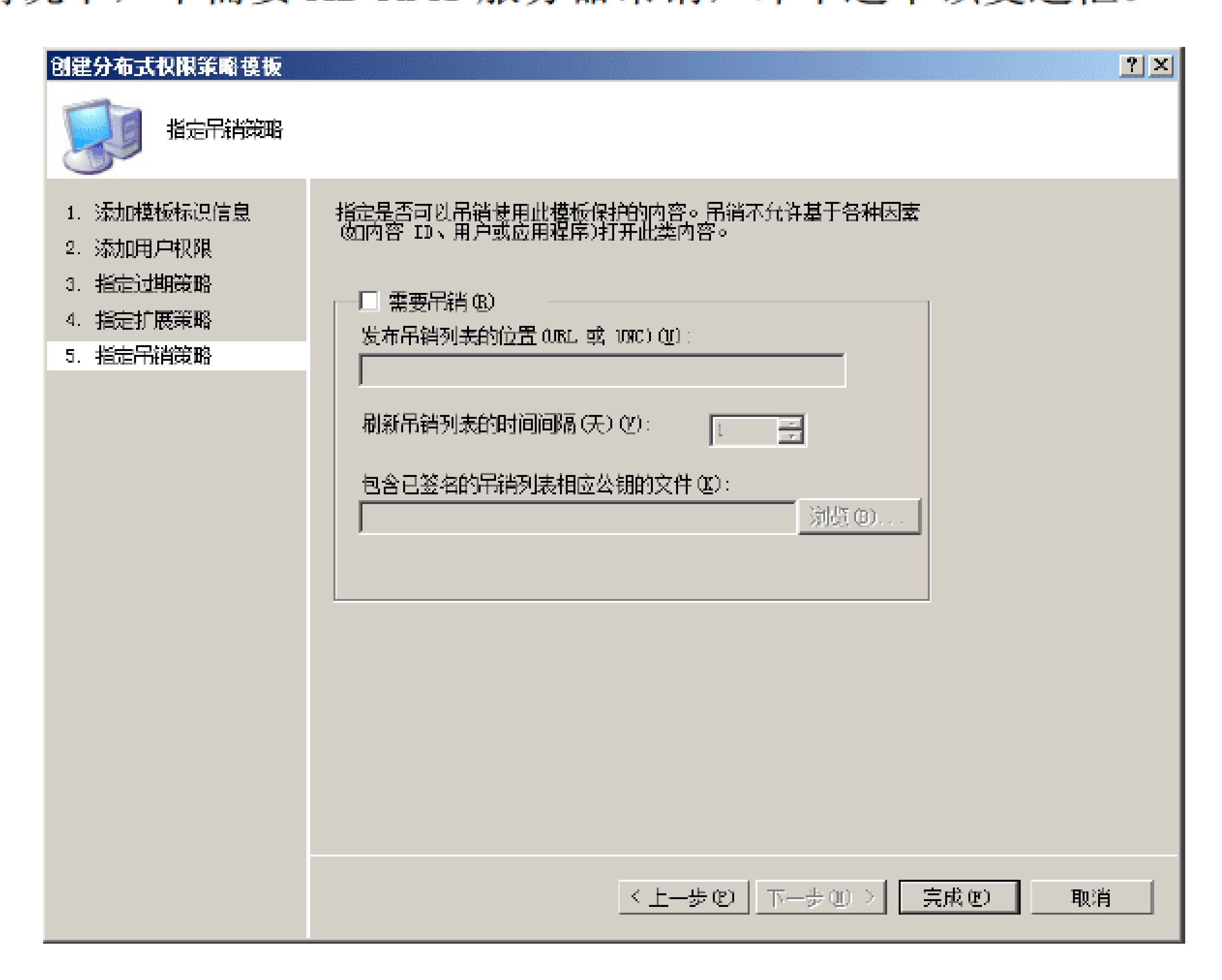


图 6-68　“指定吊销策略”界面

⑩　单击“完成”按钮，退出创建向导，返回权限策略模板窗口，如图 6-69 所示。新创建的模板已经出现在列表框中，此时虽然已经创建成功，但并不能立即应用。

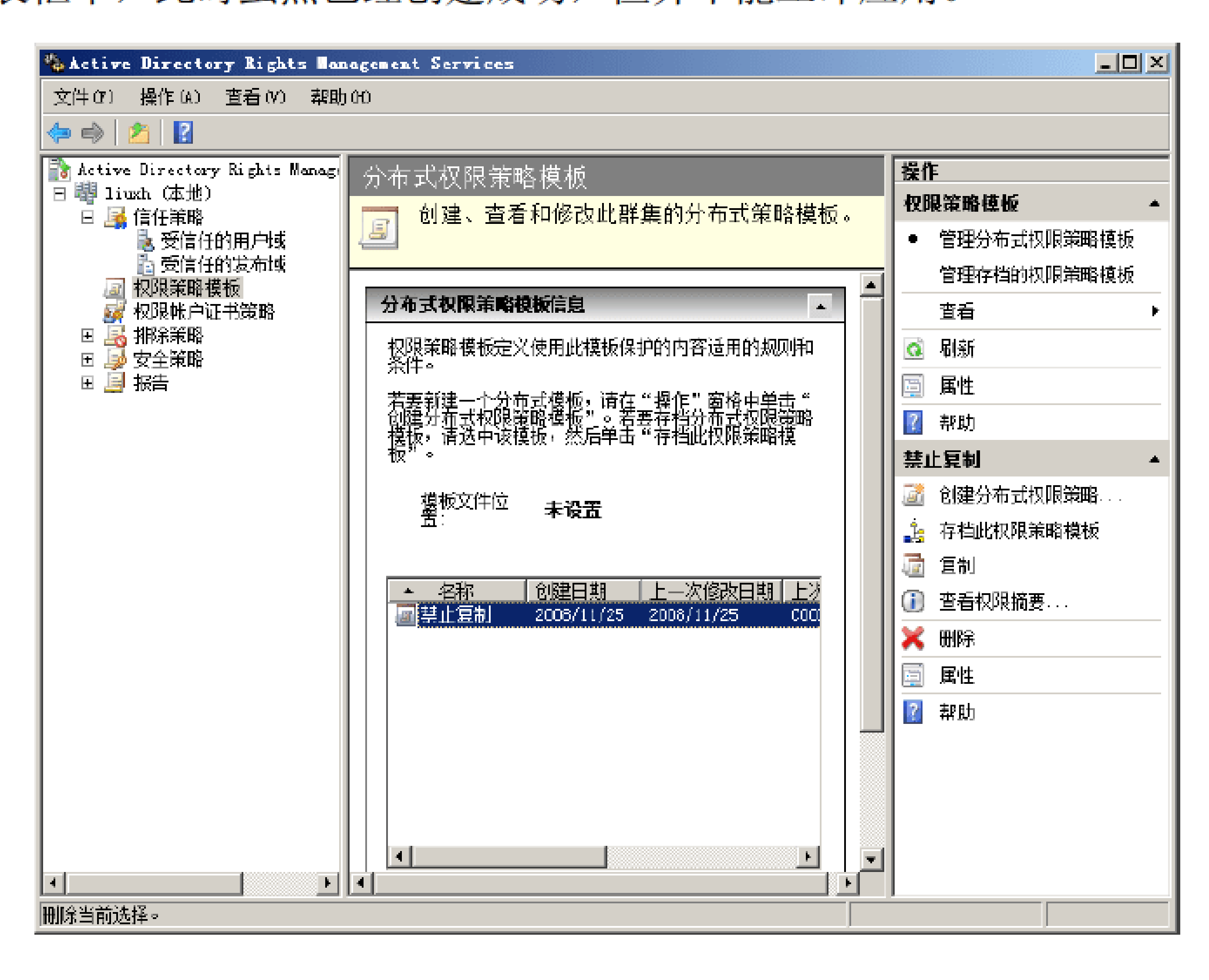


图 6-69　权限策略模板创建成功

⑪　选择新创建的策略模板，右击并选择快捷菜单中的“存档此分布式权限策略模板”命令，将其本地存档，显示如图 6-70 所示的“存档权限策略模板”对话框。提示一旦保存后，将不能再分发或导出该模板。单击“是”按钮保存即可。至此，新创建的权限策略模板才可以保存到本地模板库中备用。

⑫ 返回“分布式权限策略模板”窗口，单击“管理存档的权限策略模板”链接，所有已存档的策略模板即可显示在“公布式权限策略模板”列表框中，管理员可以继续修改和查看其各项属性信息。如图 6-71 所示是新建策略模板的权限摘要。

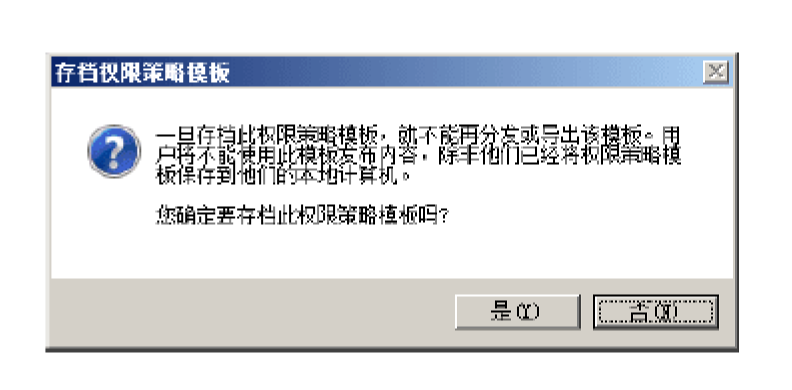


图 6-70 “存档权限策略模板”对话框

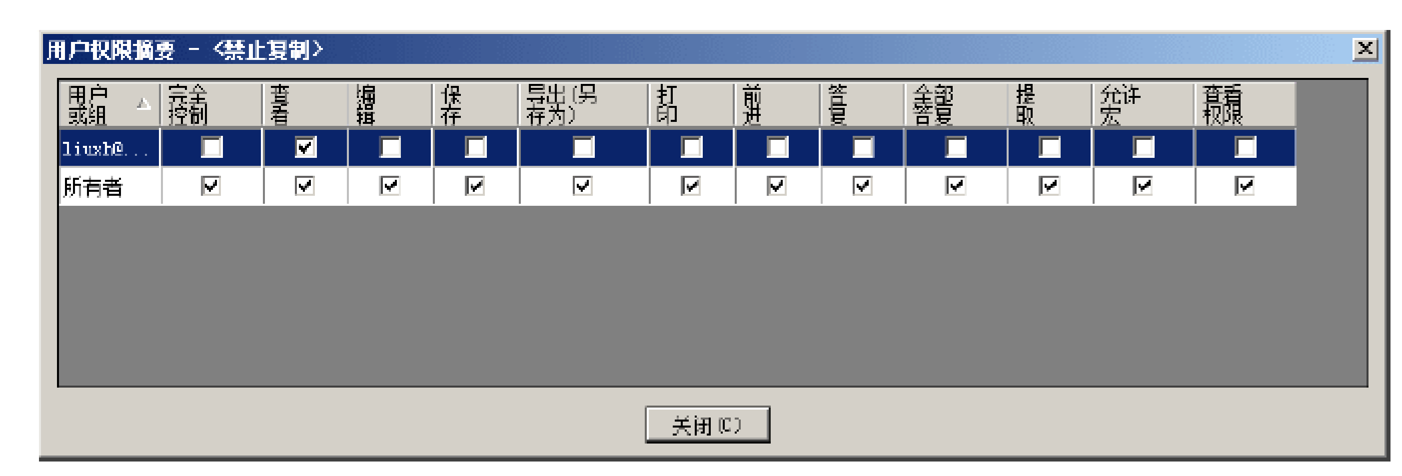


图 6-71 用户权限摘要

(2) 分发权限策略模板

客户端必须将服务器上创建的权限策略模板保存到本地计算机才可以使用，可以通过文件共享、网络传输、移动存储介质等方式获得。默认情况下，权限策略模板的保存位置为“未设置”。为了便于保存和用户使用，应在群集中指定一个公共文件夹，用于保存所有的策略模板。

① 在图 6-69 权限策略模板窗口中，单击“操作”栏中的“管理分布式权限策略模板”链接，在“分布式权限策略模板”窗格下方单击“更改分布式权限策略模板文件位置”链接，打开如图 6-72 所示的“权限策略模板”对话框。

② 选中“启用导出”复选框，在“指定模板文件位置”文本框中输入已经设置好的共享文件夹路径，如图 6-73 所示。注意，这里必须使用 UNC 格式，并且确定已经为指定用户账户赋予了写入权限。

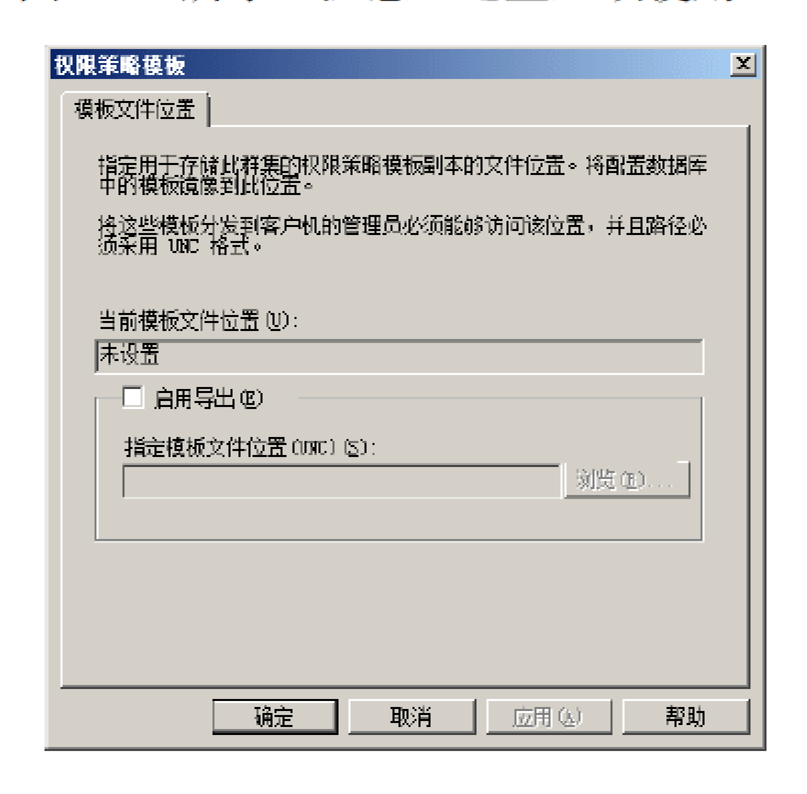


图 6-72 “权限策略模板”对话框

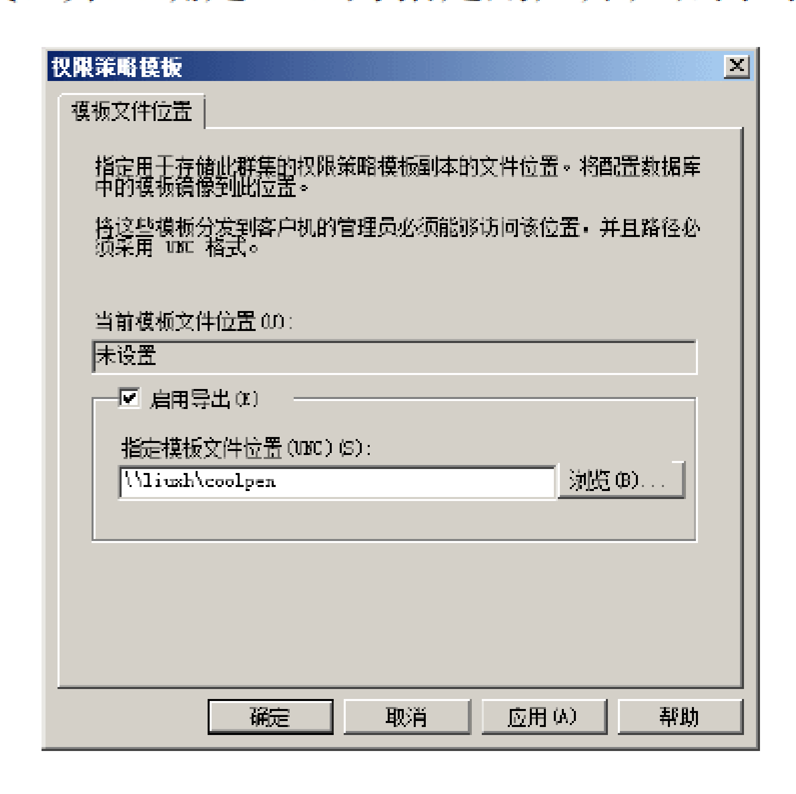


图 6-73 设置共享文件夹路径

③ 设置完成后单击“确定”按钮。然后，单击“管理存档的权限策略模板”链接，选择想要分发的模板，右击并选择快捷菜单中的“分发此权限策略模板”命令，显示如图 6-74 所示的“分发权限策略模板”对话框。提示分发之后，用户便可以使用此模板发布新内容了。

④ 单击“是”按钮确认即可。

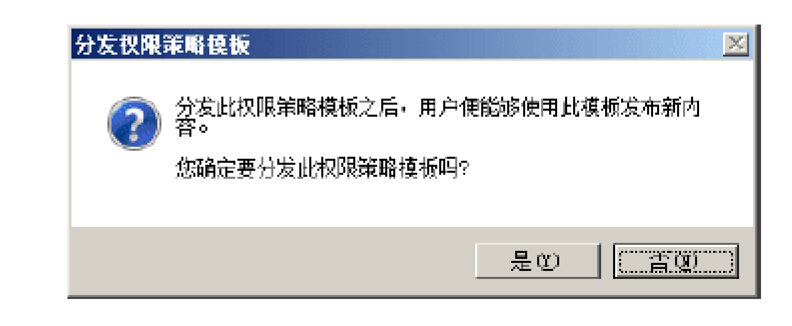
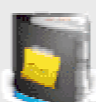


图 6-74 分发权限策略模板



提示：如果模板是从另一台 RMS 服务器迁移到此 RMS 服务器，在使用该模板之前，必须由此服务器签署，然后重新分发到客户端。

(3)　撤销权限策略模板

当某个权限策略模板不再适用时，可以将其删除。删除权限策略模板时，同时应删除用户计算机上的该模板，以便用户试图使用由已撤销的权限策略模板发布的内容时不会出现问题。当作者使用权限策略模板发布内容时，该发布请求将被发送到 RMS 服务器。RMS 将使用数据库中存储的该权限策略模板的副本来响应该请求。如果数据库中不存在该权限策略模板，请求将失败。

(4)　备份和恢复权限策略模板

要保护重要的权限策略模板，可以将配置数据库中的模板数据定期备份到媒体中，并将该媒体存放到安全的地方。这样，当系统发生故障时，管理员就可以使用备份的副本来恢复权限策略模板。

3. 配置权限账户证书策略

权限账户证书(RAC)是 AD RMS 服务器颁发给每个客户的认证凭证，该证书将用户账户与一个受保护的密钥对关联，而密钥对则专用于用户的计算机。用户可以通过这些证书来发布和使用受 AD RMS 保护的内容。每个证书都包含一个公钥，以向用户授予使用相关信息的权限。

在“AD RMS 控制台”窗口中，在左侧窗格中单击“权限账户证书策略”，显示如图 6-75 所示的“权限账户证书策略”窗格。权限账户证书根据有效期的长短和应用环境的不同，可分为标准 RAC 和临时 RAC。标准 RAC 的默认有效期限是 365 天，通常应用于固定用户的计算机上；临时 RAC 的默认有效期限为 15 分钟，主要是为了方便用户在不同位置都可以使用受 AD RMS 保护的文档。

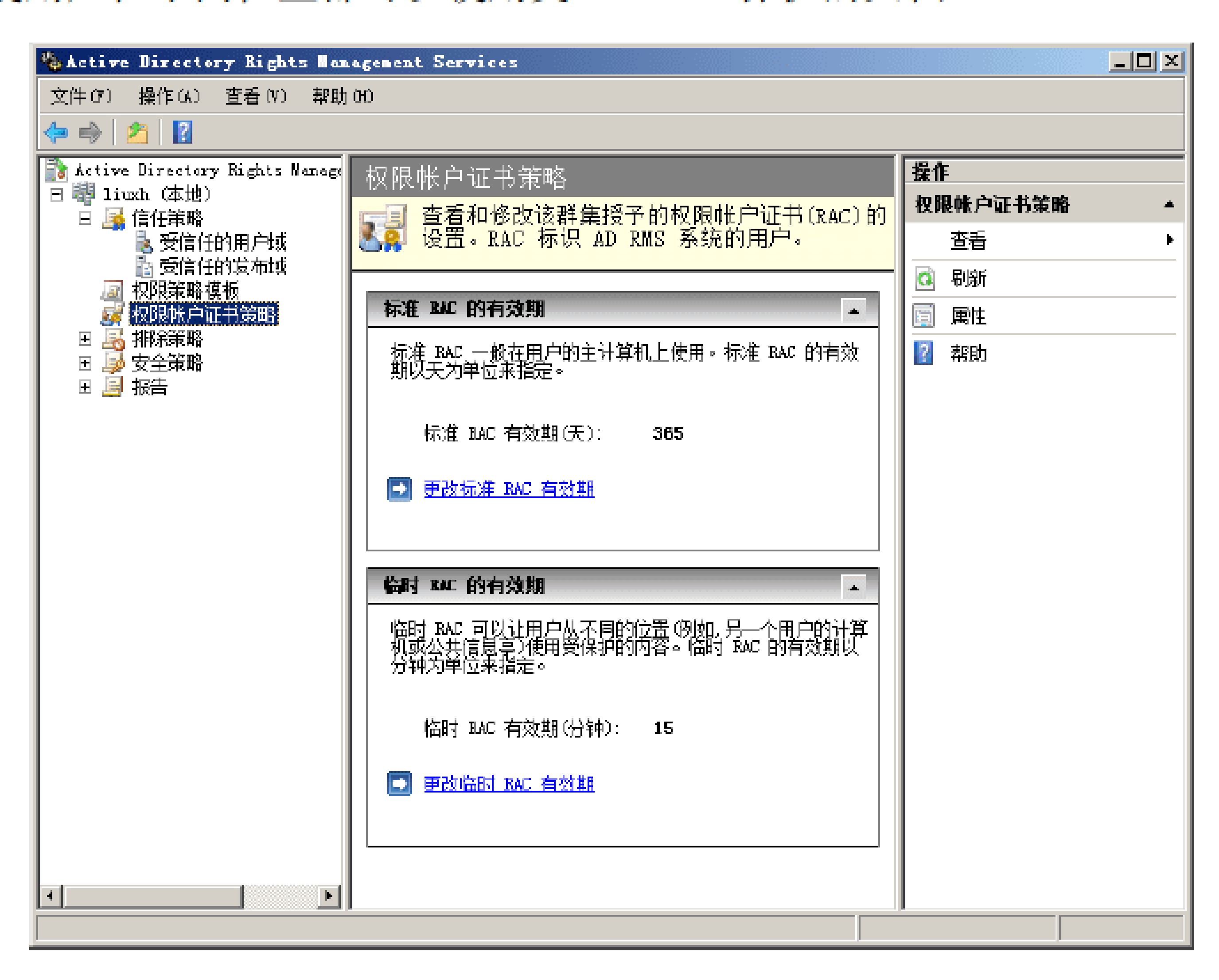


图 6-75　“权限账户证书策略”窗格

权限账户证书的有效期限可以根据实际需要更改。单击“更改标准 RAC 有效期”链接，显示如图 6-76 所示的“权限账户证书策略”对话框，在“标准 RAC 的有效期(天)”微调框中输入合适数值即可，有效期的范围是 1～9999 天。

切换到“临时 RAC”选项卡，或者在“权限账户证书策略”窗格中单击“更改临时 RAC 有效期”链接，也可以更改临时 RAC 的有效期，如图 6-77 所示。

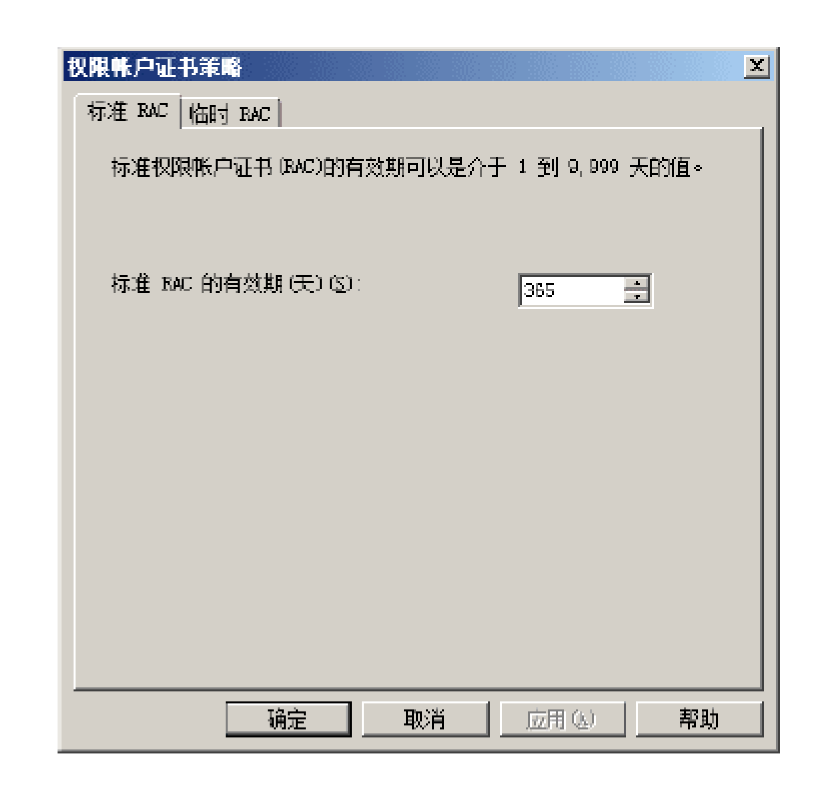


图 6-76 “权限账户证书策略”对话框

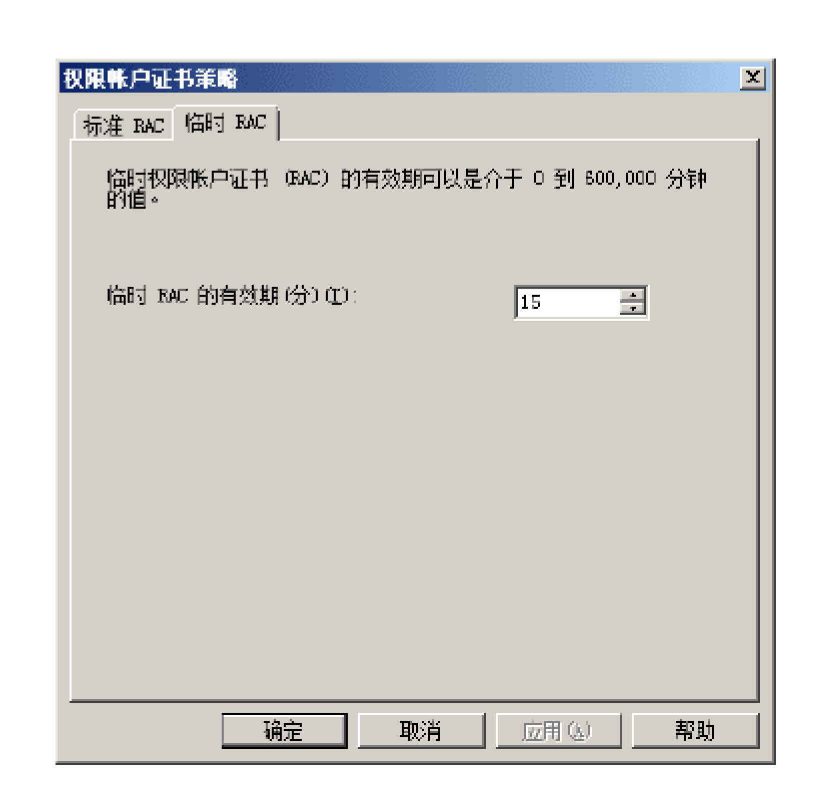
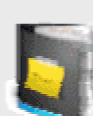


图 6-77 “临时 RAC”选项卡

6.2.4 AD RMS 客户端部署及应用

AD RMS 服务安装并配置完成以后，即可将需要接受 AD RMS 管理的客户端加入域，并部署 AD RMS 客户端。在 Windows Vista 系统中，RMS 客户端的名称已更改为 Active Directory 权限管理服务(AD RMS)客户端，并且已集成到操作系统中，因此不需要独立的安装。在早于 Windows Vista 的 Windows 操作系统版本中，RMS 客户端组件仍需要独立下载和安装。目前最新版本 SP2 简体中文版下载地址为：

```
http://www.microsoft.com/downloads/details.aspx?displaylang=zh-cn&FamilyID=02da5107-2919-414b-a5a3-3102c7447838
```



提示：管理员还可以通过组策略、SMS、SCCM 等方式来向客户端统一分发客户端安装程序。如果客户端数量较少，则可以通过手动安装的方式实现。

1. 在 Windows 2000/XP 系统中安装 RMS 客户端

AD RMS 客户端安装过程非常简单，此处不作详细介绍。需要注意的是，更换登录的域用户账户后，应重新运行客户端安装向导，并选择“修复带 Service Pack 2 的 Windows Rights Management 客户端”单选按钮。客户端需要将服务器上创建并保存的权限策略模板拷贝到自己的计算机上才可以使用，另外还需要在注册表中做相应修改。

① 通过网络共享或移动存储设备，将 AD RMS 服务器上存储的权限策略模板，复制到本地计算机上，如图 6-78 所示。

② 打开注册表编辑器，并依次展开如下分支：

```
HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Common\DRM
```

在右侧窗口空白处右击，依次选择“新建”→“字符串值”命令，新建一个字符串值项目(如图 6-79 所示)。

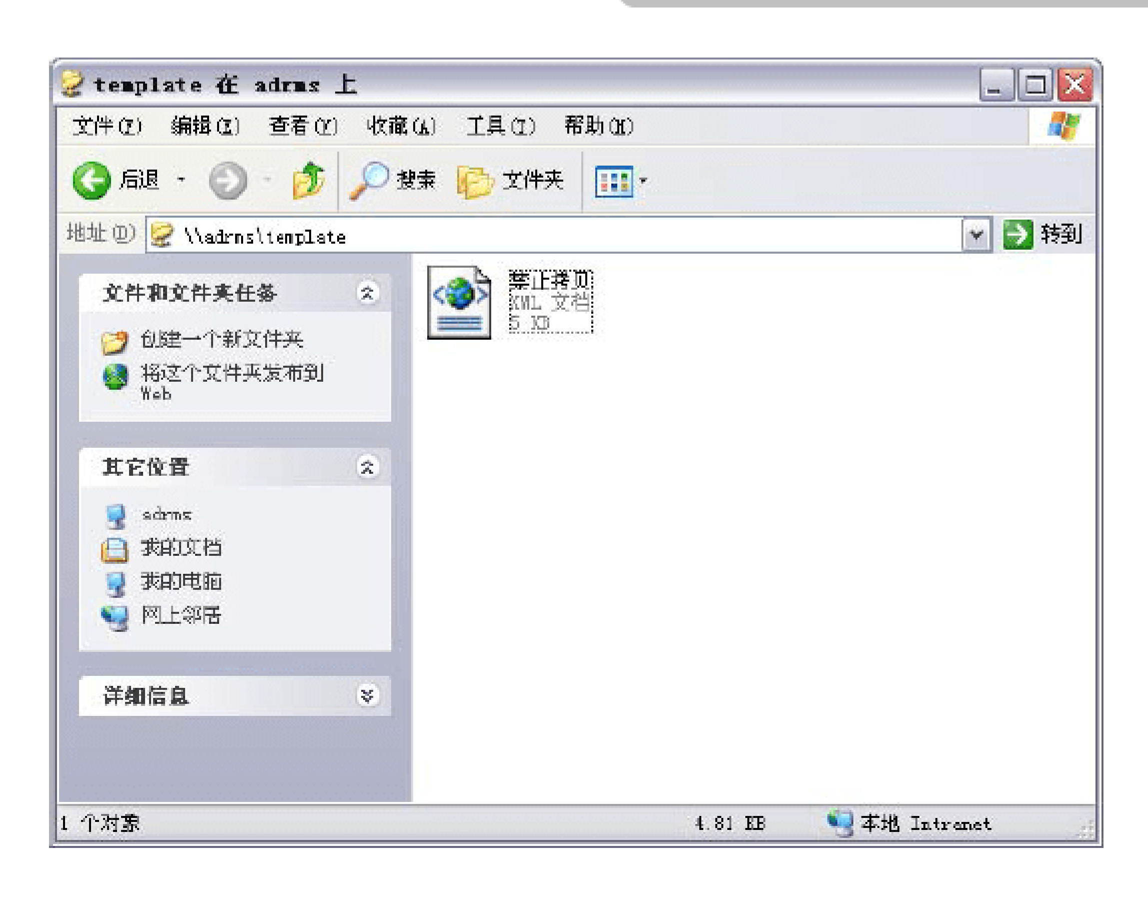


图 6-78　获取权限策略模板

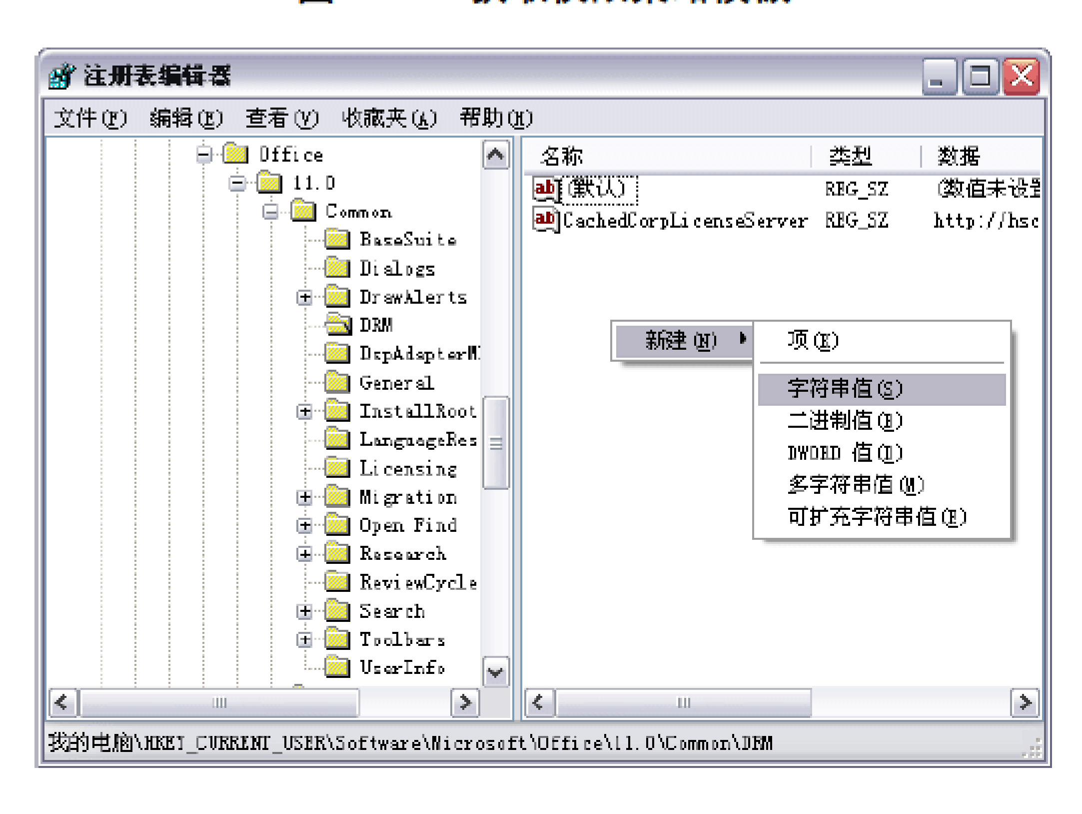


图 6-79　创建字符串值对象

③　将新创建的字符串值命名为“AdminTemplatePath”，然后双击该对象或右击选择“修改”命令打开如图 6-80 所示的“编辑字符串”对话框，指定该对象的数值数据为本地计算机上保存要应用的权限策略模板的路径。这里，将要保存在 E 盘根目录下，因此，输入“e:\”即可。

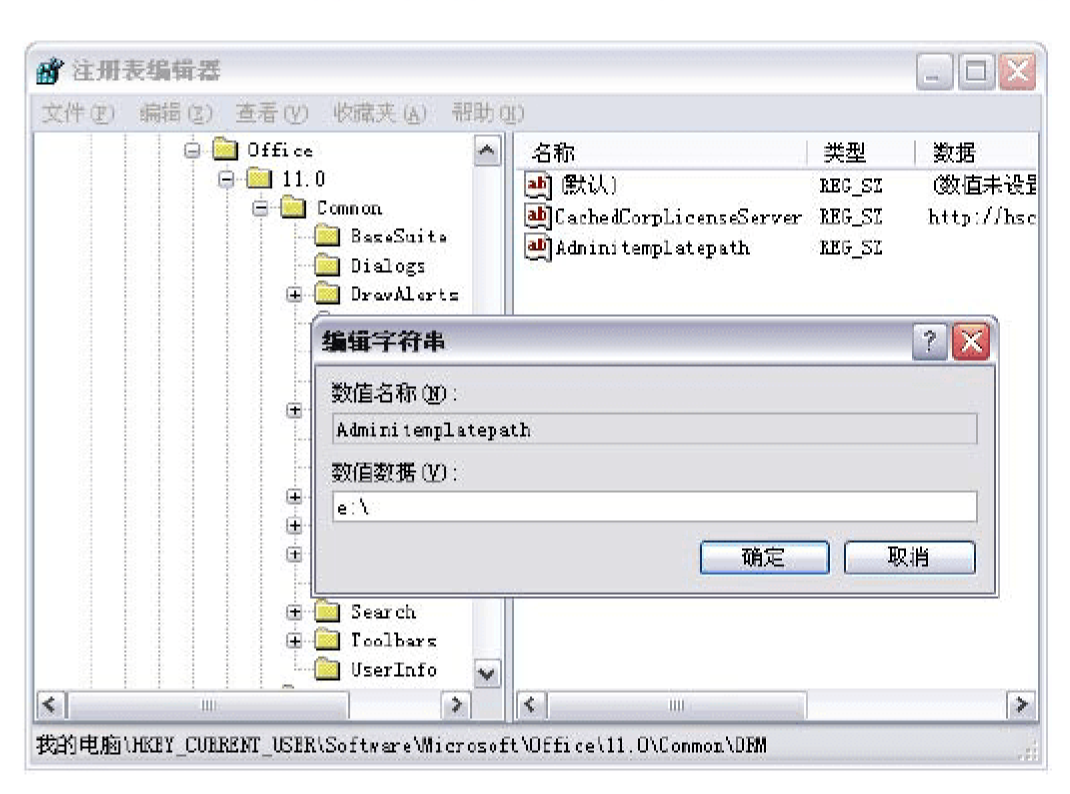


图 6-80　编辑字符串值

④　单击“确定”按钮保存设置并关闭注册表编辑器窗口。打开欲应用此策略模板的受保护文档，打

开“文件”菜单中的“权限”子菜单，此时，会发现级联菜单中多出了一个命令，即“禁止拷贝”，如图 6-81 所示。

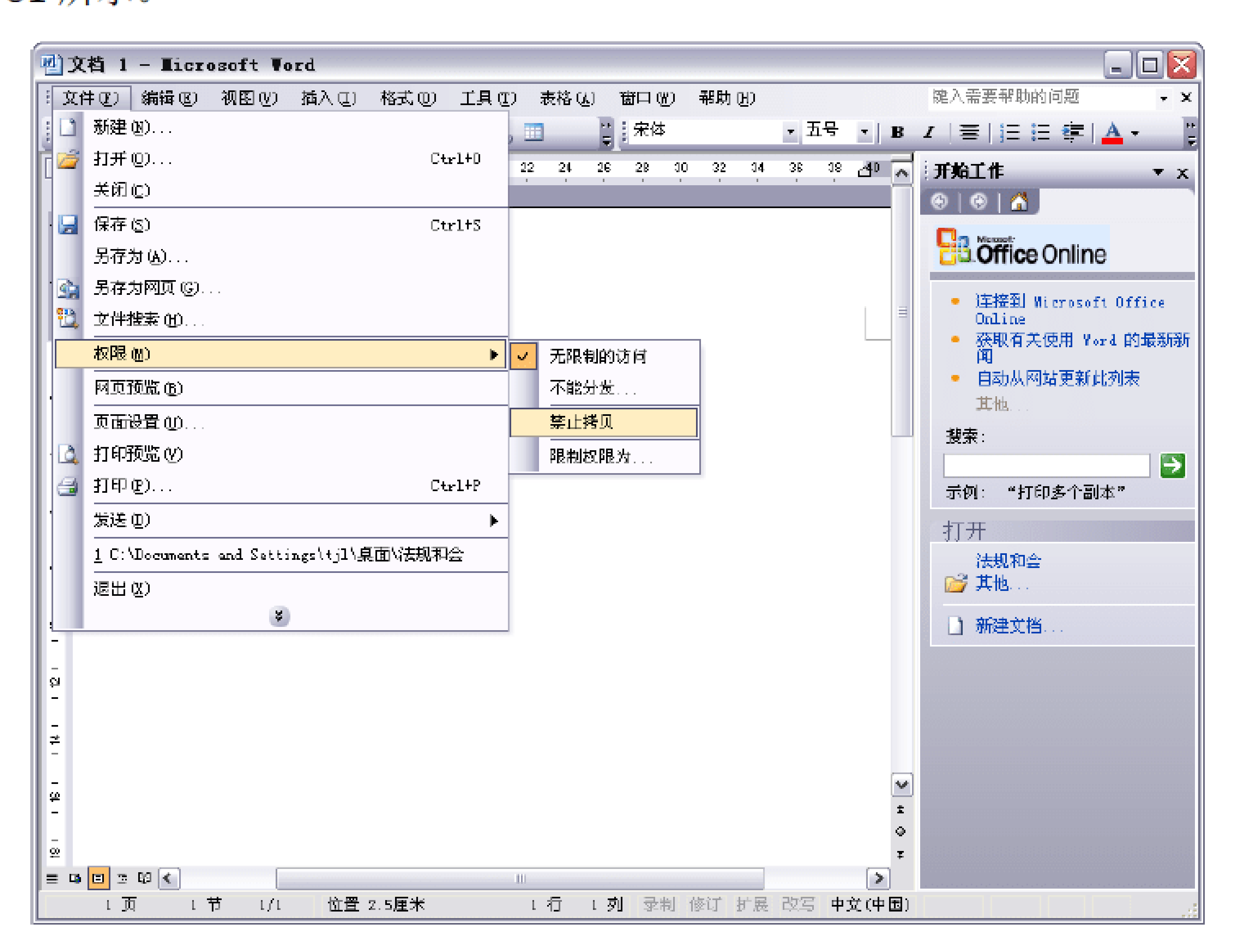


图 6-81　添加成功

⑤　选定相应策略模板后，共享工作区中会显示如图 6-82 所示的“受限权限”等信息。授权人信息默认是本地登录账户，当然，管理员也可以在建立到服务器的连接时指定为其他用户，或直接单击“更改用户”链接随时更改。本例是 lhn@coolpen.net(所用模板针对的用户为 tjl@coolpen.net)。

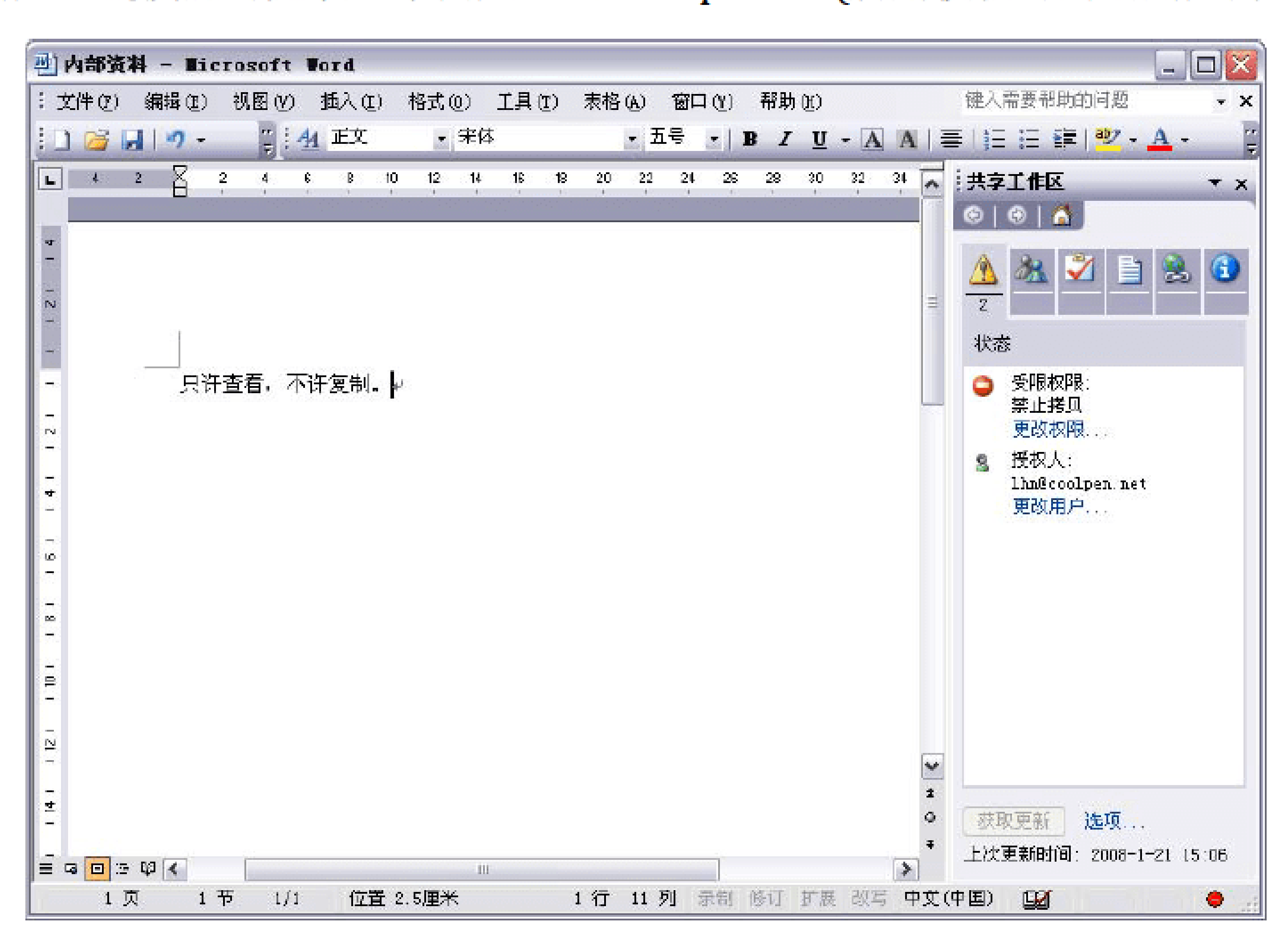


图 6-82　成功应用权限策略模板

⑥　单击共享工作区中的“更改权限”链接，可以查看当前用户账户对该文档拥有的控制权限，显示如图 6-83 所示的对话框。由于目前登录用户是该文档的创建者，在 RMS 配置该权限策略模板时，为文档作者赋予了完全控制的权限，即所有权限的状态都是“是”。

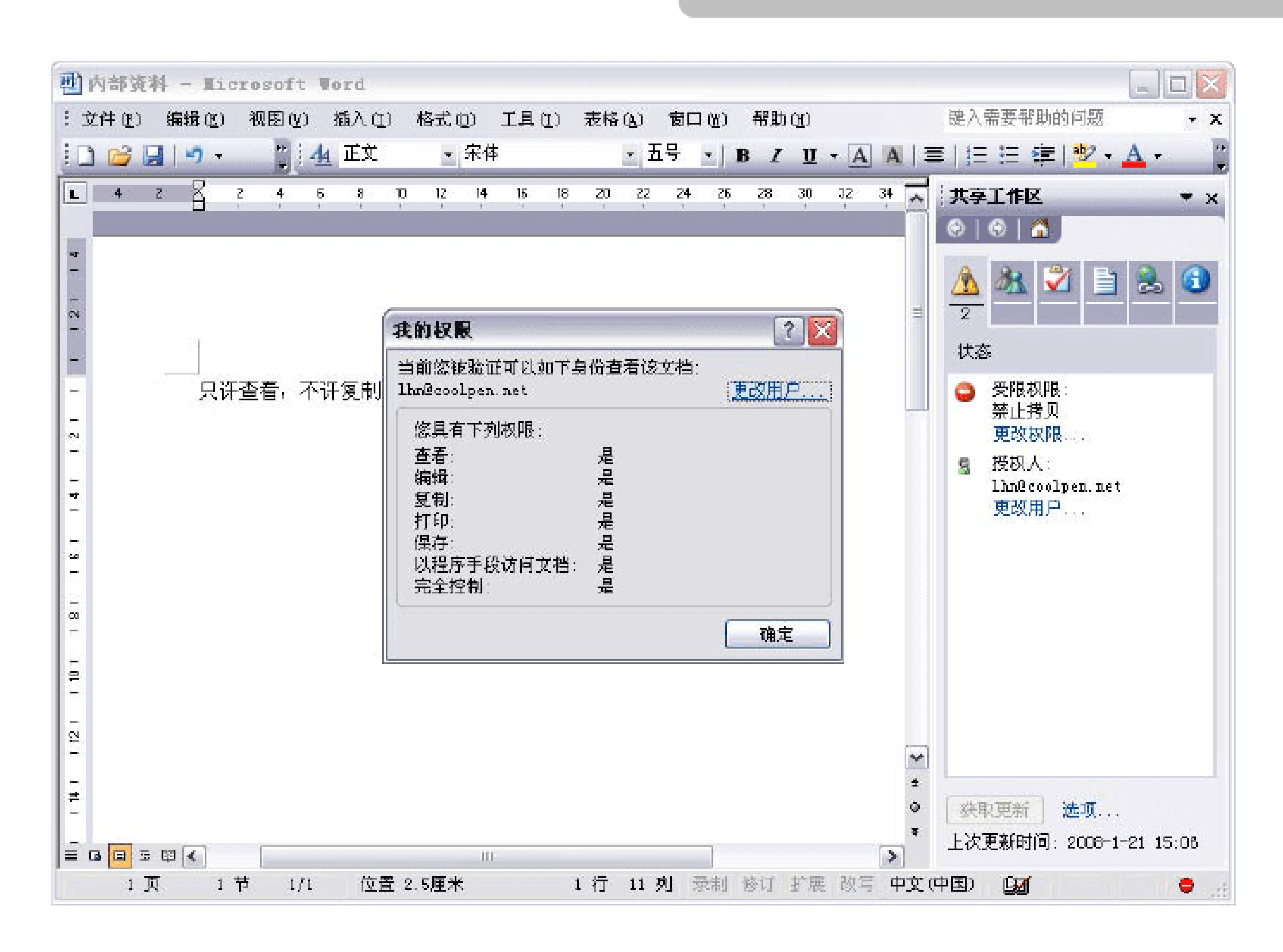


图 6-83　当前用户权限

2. 在 Windows Vista 系统中配置 AD RMS 客户端

Windows Vista 系统默认已经集成 AD RMS 客户端，用户只需进行相应配置即可使用。在 Windows 2000/XP 系统中安装 RMS 客户端之后，同样需要进行如下配置，这里以 Windows Vista 系统中的 Office Word 2007 为例加以介绍。

使用 AD RMS 服务器上策略模板中希望限制的域用户账户登录客户端计算机，如图 6-84 所示。由于该用户账户需要在本地计算机上保存策略模板，所以必须拥有对目标文件夹的写入权限。

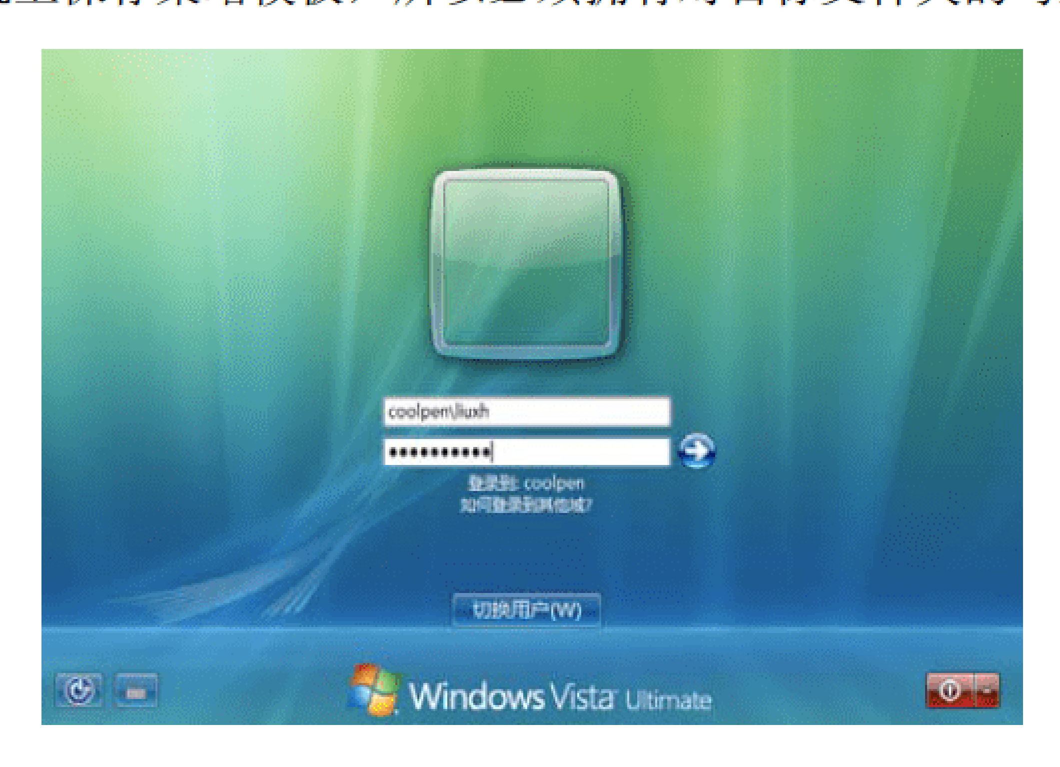


图 6-84　登录到客户端


注意：默认情况，当前登录的域用户账户将自动被添加到本地的 Users 组中，因此只需确保该组具有足够的操作权限即可。

通过网络共享或移动存储设备，将 AD RMS 服务器上存储的权限策略模板，复制到本地计算机上，并在注册表中修改相应键值，与 Windows XP 系统完全相同，此处不复赘述。应用过程也比较简单，打开欲应用此策略模板的受保护文档(以 Office Word 2007 为例)，单击“Office 按钮”并依次选择“准备”→“限制权限”选项，此时，会发现级联菜单中多出了一个可选项，即“禁止复制”，如图 6-85 所示。

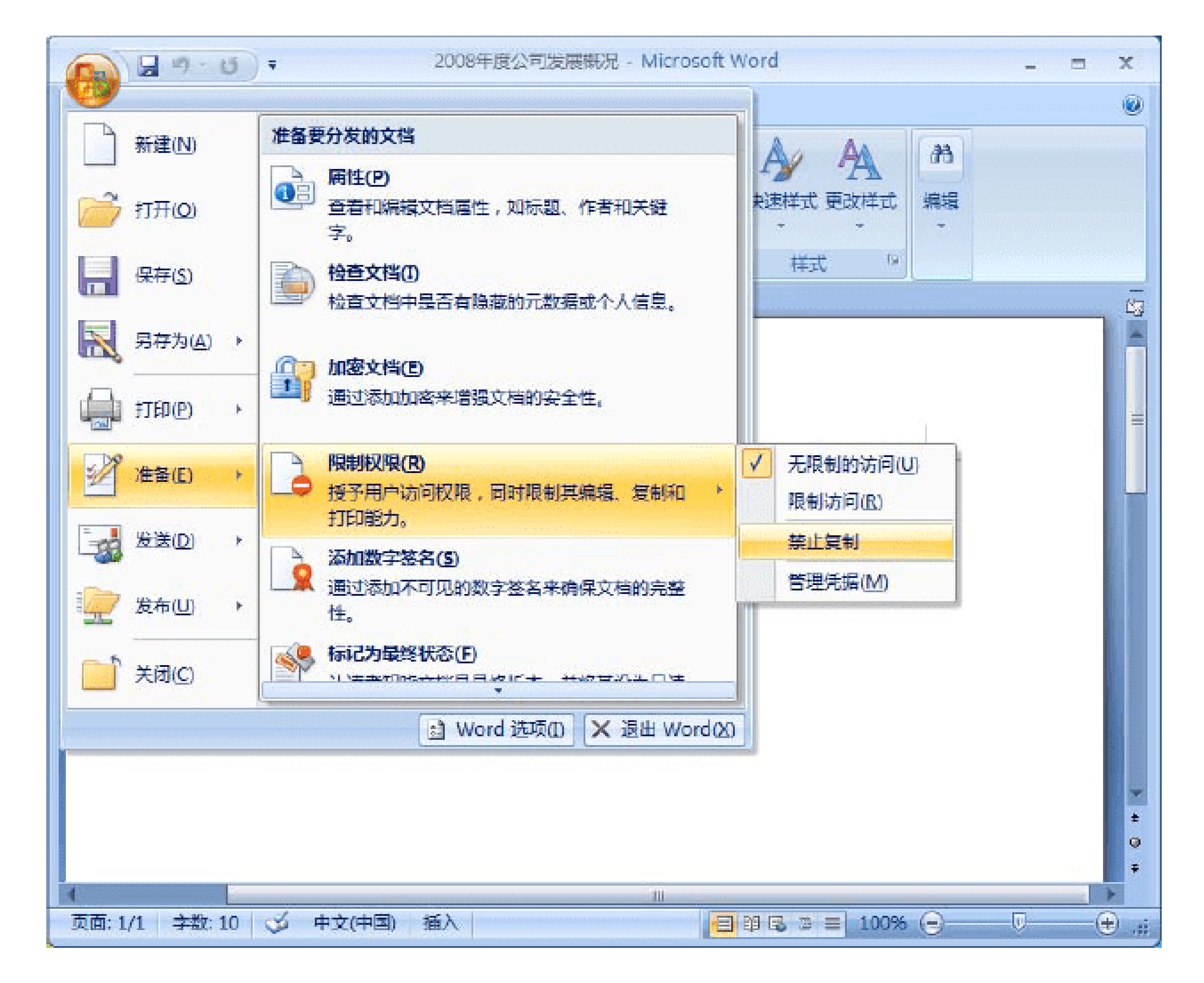


图 6-85　成功添加策略模板

3. 受限客户端应用被保护文档

AD RMS 策略模板主要是为了限制某些客户端针对文档享有的权限，因此当这些受限客户端应用被保护文档时，必须连接到 AD RMS 服务器进行凭据验证，并下载相应权限许可证才可以打开。这里，仍以上述应用为例进行介绍。



图 6-86　受限用户打开被保护文档

① 当用户 lhn@coolpen.net 创建好的文档，应用了限制用户 tjl@coolpen.net 复制和更改的权限，当用户 tjl@coolpen.net 拿到文档并查看时，会显示如图 6-86 所示的提示框。

② 单击“确定”按钮，客户端开始向 AD RMS 服务器提交身份验证，并获得相应的权限，最终打开文档，显示如图 6-87 所示窗口。不过此时，文档是“只读”状态，并且不允许用户执行“复制”命令，或按 PrintScreen 键抓取屏幕，这是因为当前被保护文档应用的权限策略模板已经屏蔽了 Windows 的这些功能，关闭受保护文档则一切恢复正常，用户使用时应注意。

③ 单击“查看我的权限”链接，打开如图 6-88 所示的“我的权限”对话框，其中只有“查看”一项处于“是”状态，其他均为“否”。

④ 单击“更改用户”链接，打开如图 6-89 所示的“选择服务”对话框，如果当前拥有的权限无法正常完成工作，可以在这里选择其中一种方式添加其他有足够权限的用户账户。选择“使用 Microsoft .NET Passport 账户”单选按钮，可以凭借有效的 Microsoft .NET Passport 账户从 Microsoft 获得一个证书，实现相应目的，这与 AD RMS 服务器的设置有关，如果添加了.NET Passport 类型的可信任用户域，则客户端可以使用这种方式，否则无效。选择“使用 Microsoft Windows 账户”单选按钮，即可从当前域中选择其他用户账户来完成相应操作。

如果上述方法仍不能获得相应权限，则可以在“我的权限”对话框中，单击“请求附加权限”链接，向 AD RMS 服务器申请相关权限，打开如图 6-90 所示的窗口。“收件人”文本框中就是 AD RMS 服务器上设定的接收申请的电子邮件地址，保持默认即可。根据自己的实际需要，说明想要请求的权限即可。

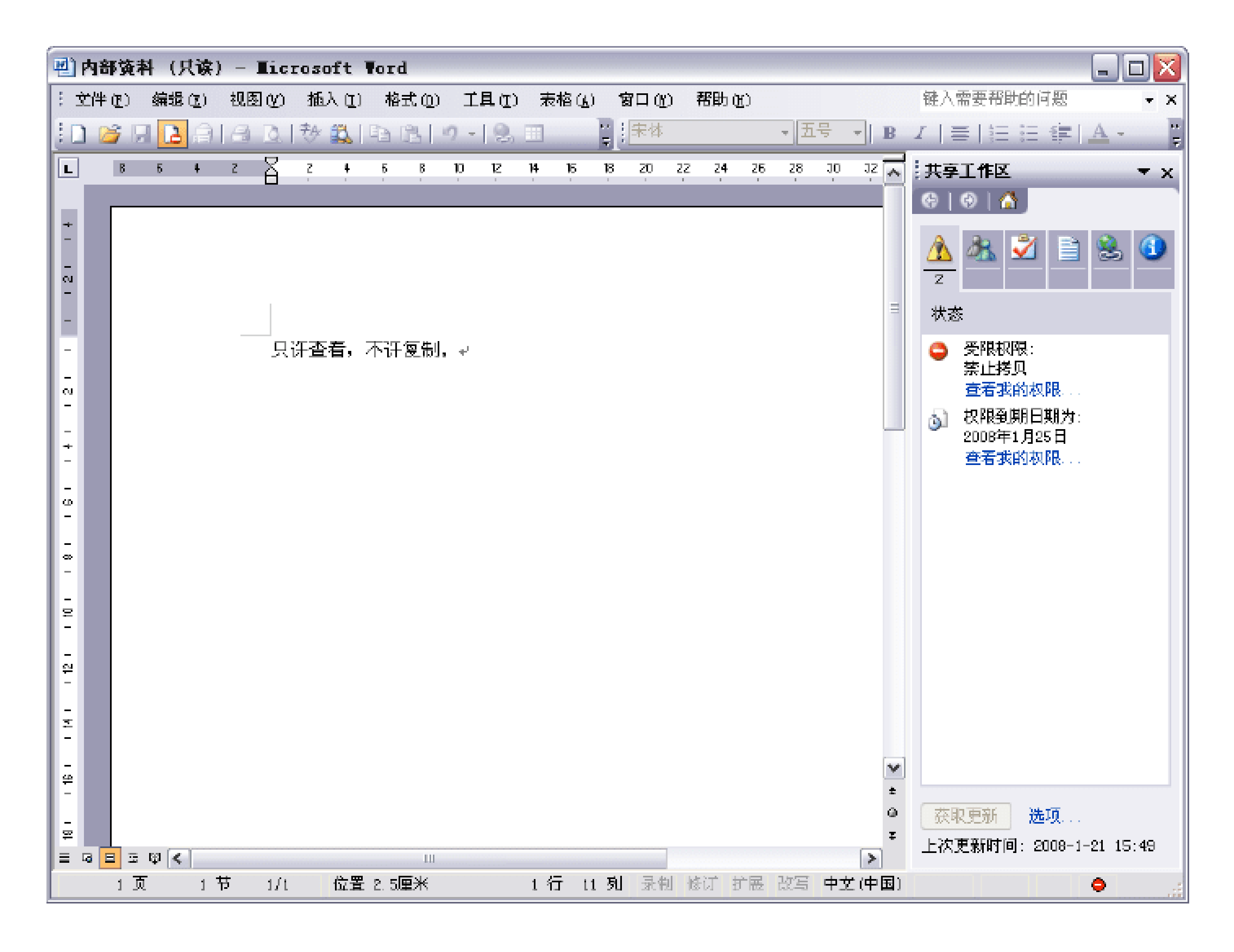


图 6-87　文档处于“只读”状态

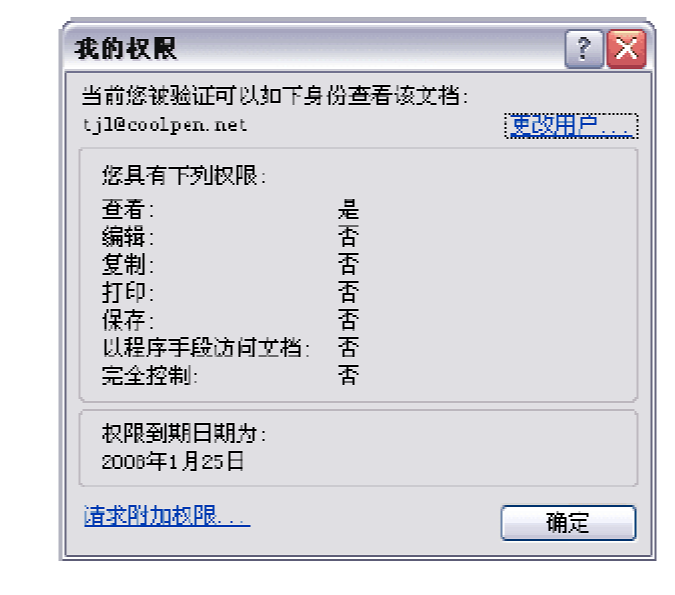


图 6-88　“我的权限”对话框

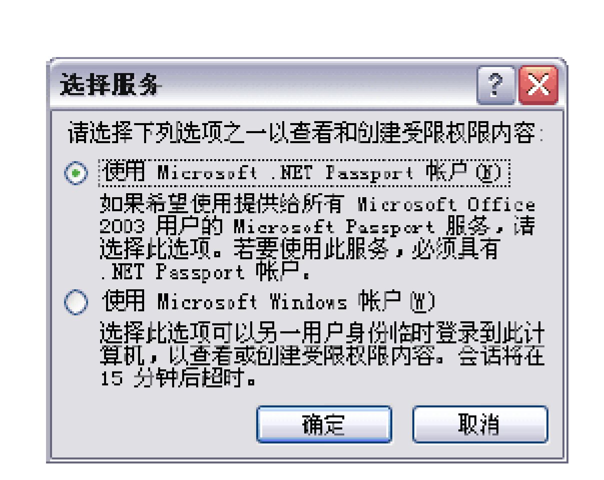


图 6-89　“选择服务”对话框

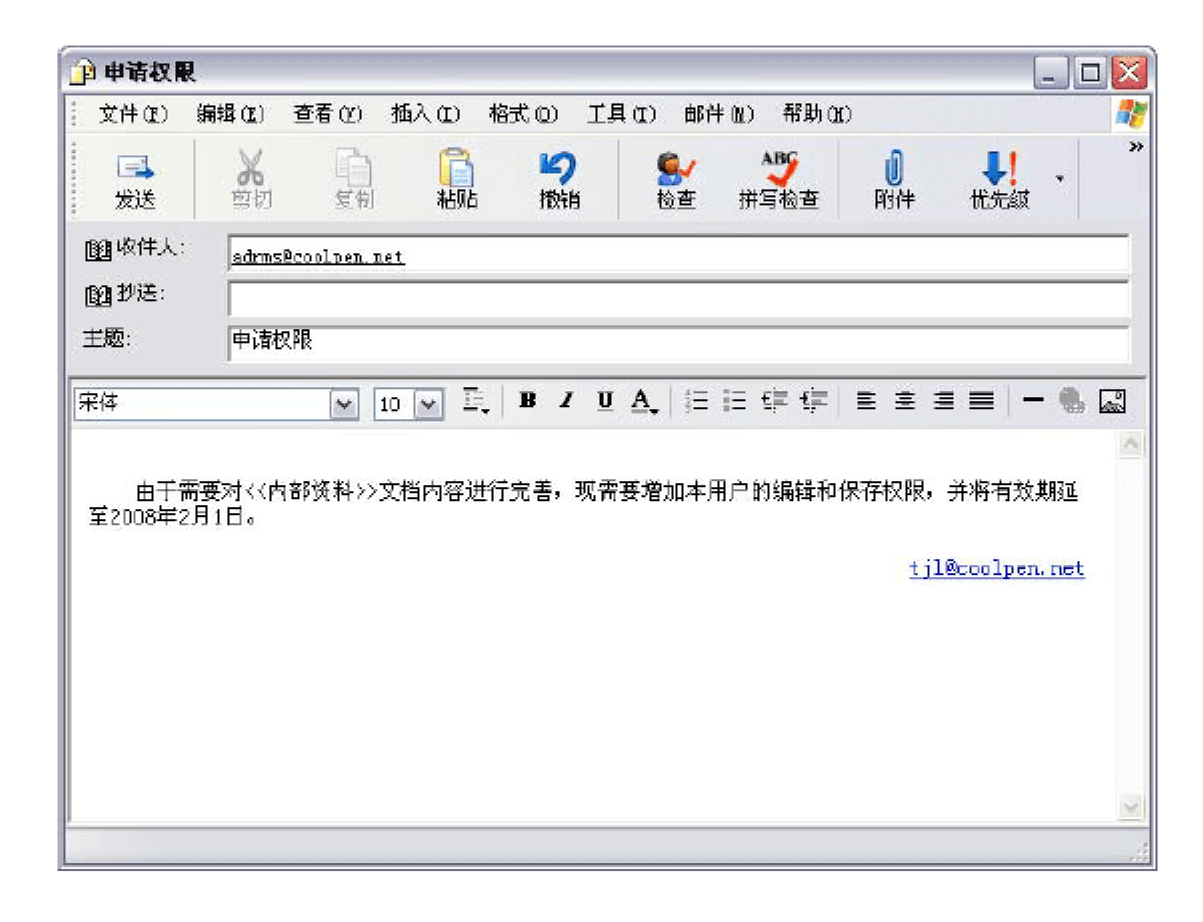


图 6-90　申请附加权限



提示：需要应用此功能时，必须先在网络中配置 Exchange 或其他邮件服务器。虽然在 AD RMS 系统中用到 E-mail 地址的地方非常多，但是多数情况下是作为一种用户标识，并非真正的用来传递信息，所以网络中邮件服务器也就可有可无。如果确实需要传递信息，则必须搭建邮件服务器。

6.3　共享资源安全

通常情况下，共享资源是面向网络中的所有用户的，即任何进入网络的用户都可以查看或使用共享资源。保护共享资源，实现安全访问是局域网安全中必不可少的，最常用的方法就是限制赋予用户的访问权

限。前面介绍的保护本地文件安全的方法同样适用于共享资源，并且优先于共享权限。对于安全性要求较高的共享资源，可以同时采用多种安全限制措施。

6.3.1 管理共享文件夹权限

当将文件夹设置为共享资源时，除了必须为文件和文件夹指定 NTFS 权限外，还应当为共享文件夹指定相应的访问权限。共享文件夹权限比 NTFS 权限简单一些，而且 NTFS 权限的优先级要高于共享文件夹权限。因此，共享文件夹的权限可以粗略设置，而 NTFS 权限则必须详细划分。

1. 设置共享权限

由于网络用户对文件资源的访问都是通过网络共享实现的，所以，除了设置 NTFS 权限外，还需要设置共享文件夹权限。

在共享文件夹“属性”对话框的“共享”选项卡中，单击“权限”按钮，即可显示共享文件夹的权限对话框，显示并设置该共享文件夹的权限，如图 6-91 所示。

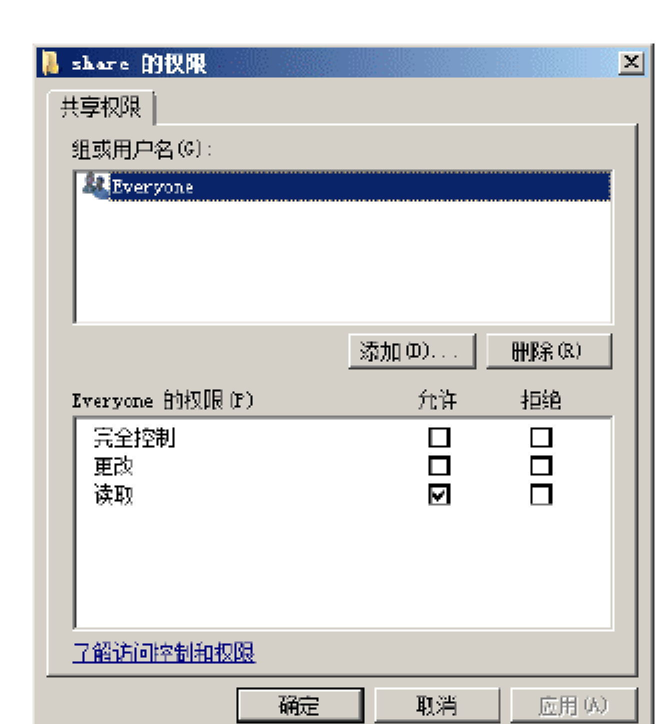


图 6-91 共享文件夹的权限对话框

共享文件夹权限具有以下特点：

- 共享文件夹权限只适用于文件夹，而不适用于单独的文件，并且只能为整个共享文件夹设置共享权限，而不能对该共享文件夹中的文件或子文件夹进行设置。所以，共享文件夹权限不如 NTFS 文件系统权限详细。
- 共享文件夹权限并不对直接登录到计算机上的用户起作用，它们只适用于通过网络连接该文件夹的用户。也就是说，共享权限对直接登录到服务器上的用户是无效的。
- 在 FAT/FAT32 系统卷上，共享文件夹权限是保证网络资源被安全访问的唯一方法。原因很简单，NTFS 权限不适用于 FAT/FAT32 卷。
- 默认的共享文件夹权限是读取，并被指定给 Everyone 组。

共享权限分为读取、修改和完全控制。不同权限以及对用户访问能力的控制如表 6-4 所示。

表 6-4 共享权限对应的操作

权 限	允许用户完成的操作
读取	显示文件夹名称、文件名称、文件数据和属性，运行应用程序文件，以及改变共享文件夹内的文件夹
修改	创建文件夹，向文件夹中添加文件，修改文件中的数据，向文件中追加数据，修改文件属性，删除文件夹和文件，以及执行“读取”权限所允许的操作
完全控制	修改文件权限，获得文件的所有权 执行“修改”和“读取”权限所允许的所有任务。默认情况下，Everyone 组具有该权限

共享文件夹权限的多重权限与 NTFS 文件系统权限相似，这里不复赘述。

在管理共享文件夹和指定共享文件夹权限时，应当遵守以下策略：

- 确定每个资源有哪些组需要访问，以及这些组对每个资源各自不同的权限级别。
- 为组而不是用户指定权限，以简化访问管理。

- 为资源指定最严格的权限，只要允许用户完成所需要的任务即可。
- 在组织资源时，将对安全性要求相同的文件夹放在一个文件夹中。例如，如果用户需要拥有几个文件夹的读取权限，那么，最好将这些应用文件夹存放在同一文件夹，然后再共享这个文件夹，而不是单独地共享每个文件夹。
- 使用一目了然的直观的共享名，便于用户识别并找到所需要的资源。

2. 共享权限与 NTFS 权限

如何快速有效地控制对 NTFS 磁盘分区上网络资源的访问呢？答案就是利用默认的共享文件夹权限共享文件夹，然后通过授予 NTFS 权限控制对这些文件夹的访问。当共享的文件夹位于一个利用 NTFS 格式化的磁盘分区上时，该共享文件夹的权限即与 NTFS 权限进行组合，用以保护文件资源。共享文件夹为资源提供有限的安全性，而 NTFS 权限为共享文件夹提供最大的灵活性。不论是在本地访问资源，还是通过网络访问该资源，NTFS 权限都起作用。

当在 NTFS 卷上为共享文件夹授予权限时，应当遵守下述规则：

- 可以对共享文件夹中的文件和子文件夹应用 NTFS 权限。可以对共享文件夹中包含的每个文件和子文件夹应用不同的 NTFS 权限。
- 除共享文件夹权限外，用户必须要有该共享文件夹包含的文件和子文件夹的 NTFS 权限，才能访问那些文件和子文件夹。在 FAT 卷上，共享文件夹权限是保护该共享文件夹中的文件和子文件夹的唯一权限。
- 在 NTFS 卷上必须要求有 NTFS 权限。默认情况下，Everyone 组具有“完全控制”权限。

当对 NTFS 权限和共享文件夹的权限进行组合时，组合结果所产生的权限或者是组合的 NTFS 权限，或者是组合的共享文件夹权限，哪个范围更窄、哪个权限更严格就是哪一个。例如，Users 对 Public 共享文件夹的完全控制权限，但只对其中的 File1 拥有只读权限。那么，应当设置 User 拥有对共享文件夹 Public 完全控制的共享权限。在设置 Public 的 NTFS 权限时，也设置 Users 对 Public 的完全控制权限，同时，将 File1 设置为读取权限，如图 6-92 所示。

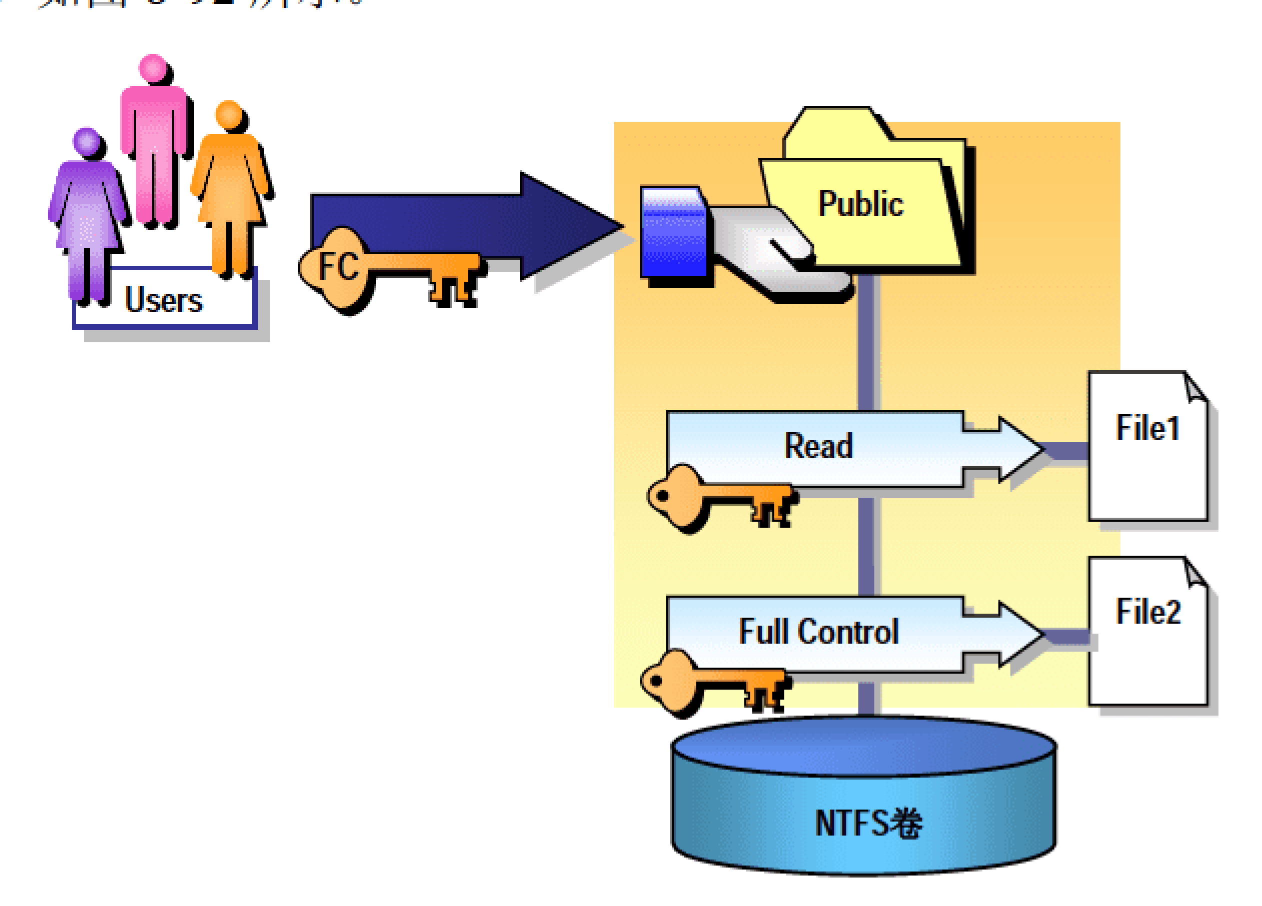
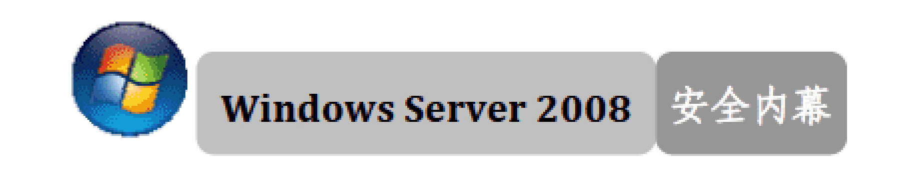


图 6-92　NTFS 权限的优先级

3. Windows Server 2008 共享和发现

共享和发现是 Windows Server 2008 系统集中管理局域网共享的方式之一，主要包括网络发现、文件



共享、打印机共享、密码保护的共享等几项。

(1) 网络发现

通过配置“网络发现”功能，可以将自己的计算机暴露在局域网中，或者从局域网中隐藏，不被其他用户发现。开启“网络发现”功能，则可以自动发现网络中的其他启用“网络发现”功能的 Windows Server 2008 和其他服务器，关闭则无法发现其他计算机。需要注意的是，关闭“网络发现”功能时，其他计算机仍可以通过搜索或指定计算机名、IP 地址的方式访问到该计算机，但不会显示在其他用户的“网络”中。

为了便于服务器之间的互访建议开启此功能，单击“网络发现”右侧的下拉三角按钮展开，选择“启用网络发现”单选按钮，并单击“应用”按钮即可，如图 6-93 所示。

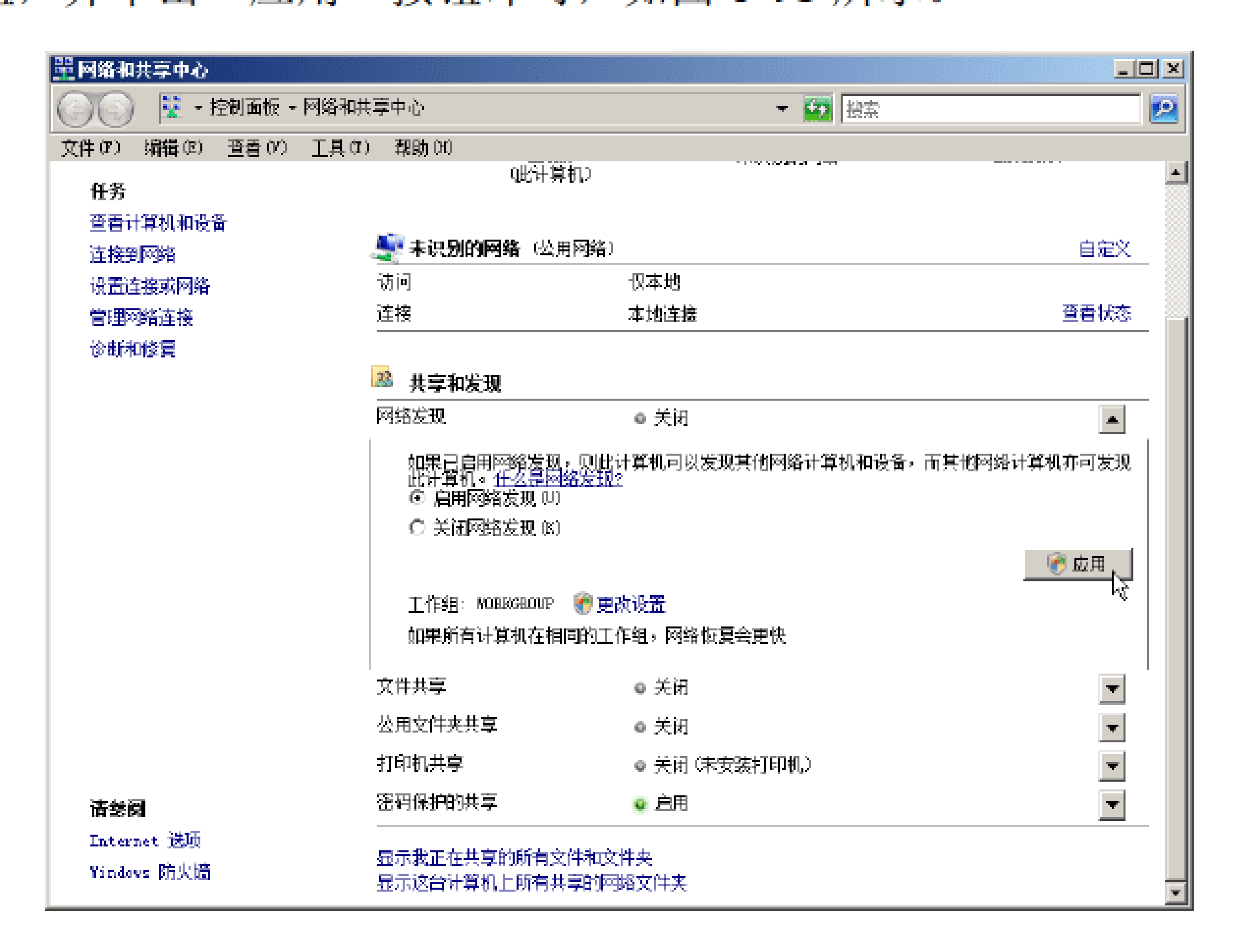


图 6-93 网络发现

(2) 密码保护的共享

如果启用密码保护功能，则其他用户必须具备当前计算机的用户账户和密码才可以访问已经共享的资源，如果已经加入域中，则必须凭借有足够权限的域用户账户才可以连接到此计算机的共享资源。Windows Server 2008 默认是启用该功能的，如图 6-94 所示。



图 6-94 密码保护的共享

6.3.2　默认共享安全

默认共享主要是为了方便网络管理员管理网络中的计算机，特别是在基于域的网络中，专门有几个默认共享用于存储用户配置文件是非常方便的。但是，默认共享在方便管理的同时，也给计算机的安全埋下了重大安全隐患。如果知道了管理员账户和密码，任何人都能访问计算机，所以如果管理员账户密码被恶意用户窃取，对于计算机的安全来说是非常不利的。

1.　查看默认共享

默认共享是为了方便管理员远程管理而默认开启的共享(当然可以关闭它)，即所有的逻辑磁盘(C$、D$、E$……)和系统目录 Windows NT 或 Windows(ADMIN$)，通过 IPC$连接可以实现对这些默认共享的访问。

(1)　命令行方式

如果想要查看本地计算机目前所打开的默认共享，可以在本地计算机的命令提示符下，使用 Net share 命令来查看系统目前所有的共享的目录。在这些所列出的共享目录中，不但包括默认共享，还包括系统除默认共享以外的所有共享目录。

具体操作过程如下。

在命令行提示符下，输入：

```
Net share
```

按 Enter 键，命令成功执行，如图 6-95 所示。

在这里所显示就是系统的所有共享目录，这里主要包括 IPC$默认共享、逻辑磁盘共享“D$、C$”，系统目录共享“ADMIN$”。

(2)　图形窗口方式

如果用户对在命令提示符下的操作不是很熟悉的话，还可以使用图形方式，查看目前系统的默认共享目录。

①　以管理员账户登录系统，依次选择“开始”→“管理工具”→“计算机管理”选项，打开“计算机管理”窗口，如图 6-96 所示。

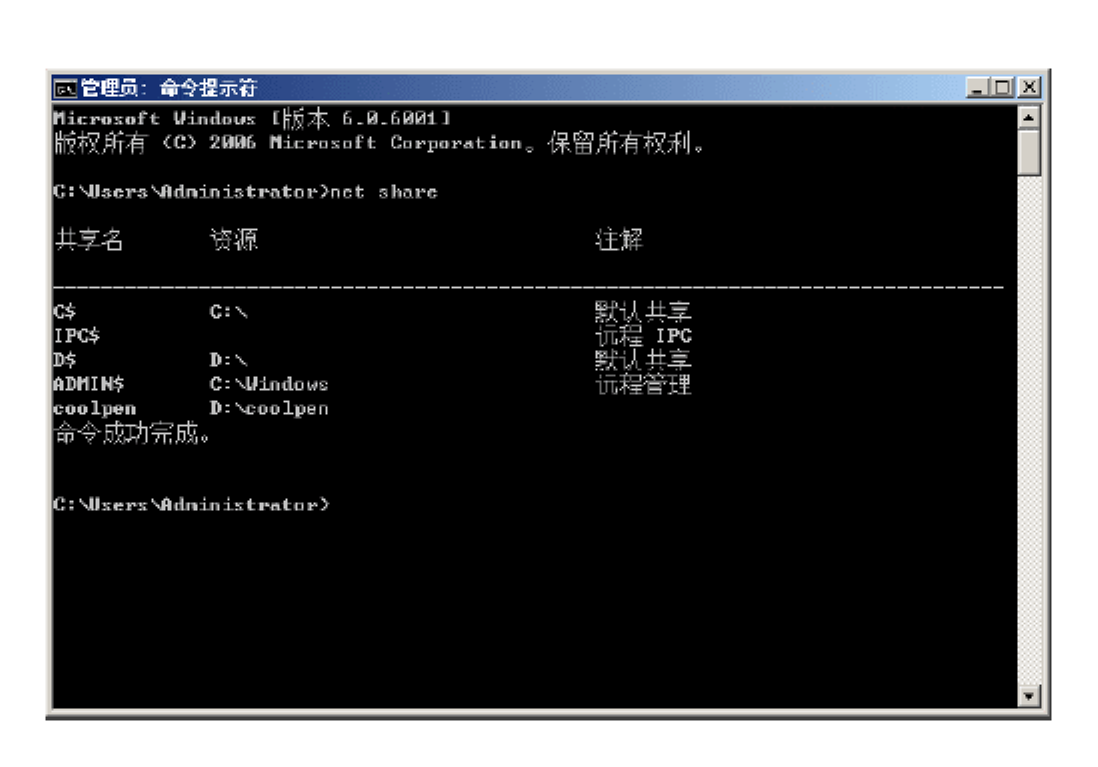


图 6-95　Net share 的执行结果

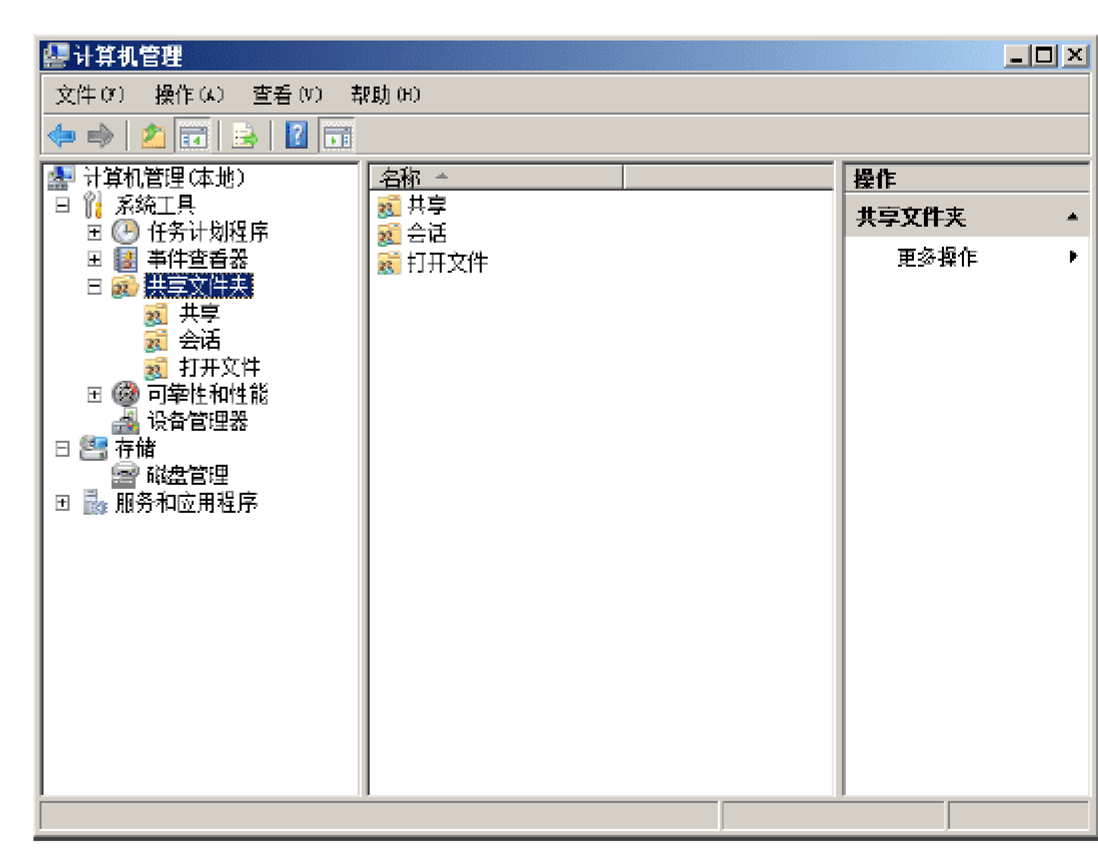


图 6-96　“计算机管理”窗口

② 在“计算机管理”窗口左侧的“计算机管理”列表树中，依次展开“系统工具”→“共享文件夹”→“共享”选项，如图 6-97 所示。

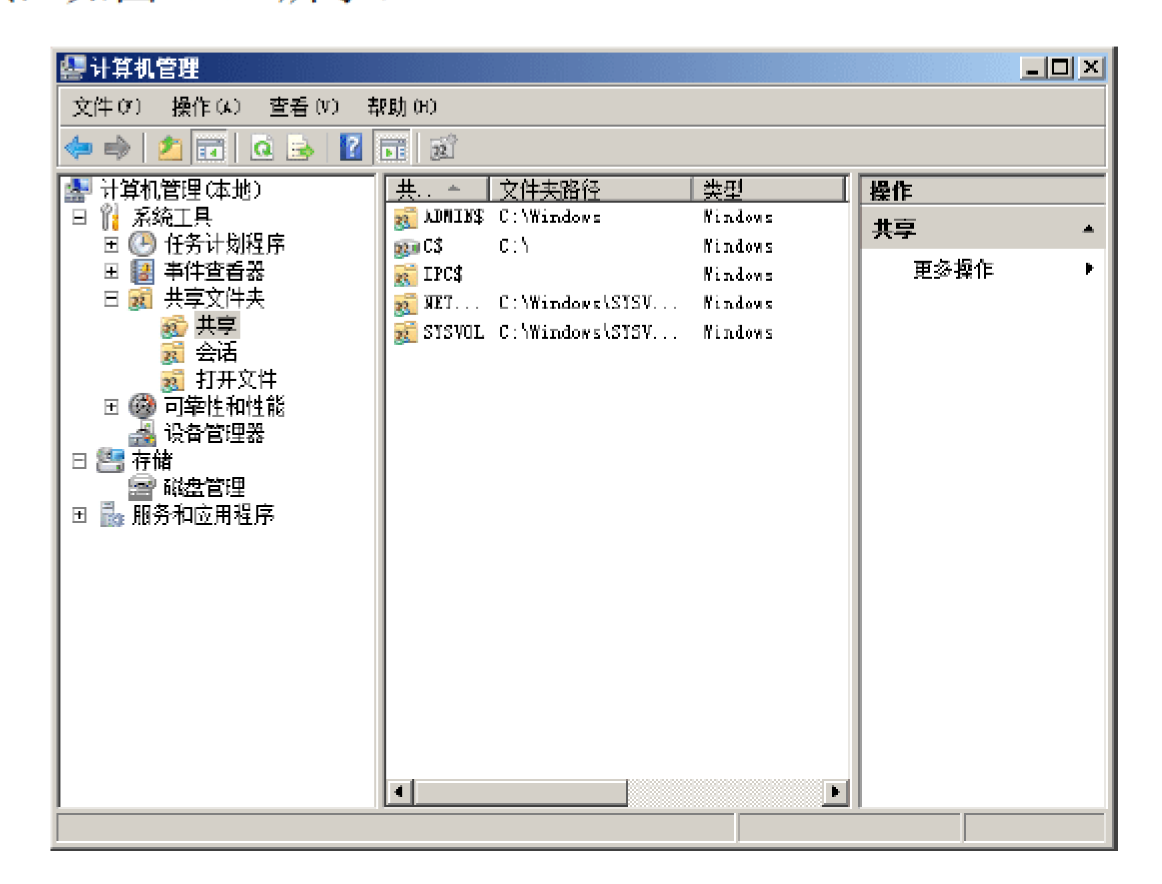


图 6-97 共享文件夹

③ 选择“共享”选项，在右侧的共享列表中，可以查看本地计算机上已经设置的默认共享。

2. 停止默认共享

如果在网络中没有使用默认共享的必要，建议用户将系统的默认共享关闭，从而进一步的保证计算机的安全。

(1) 使用 Net share 命令

首先，介绍如何在命令提示符下，使用命令停止系统的默认共享，所使用的命令为“Net share”。

具体操作过程如下。

在命令行提示符下，输入：

```
net share d$ /delete
```

按 Enter 键，命令成功执行，即可停止共享，如图 6-98 所示。

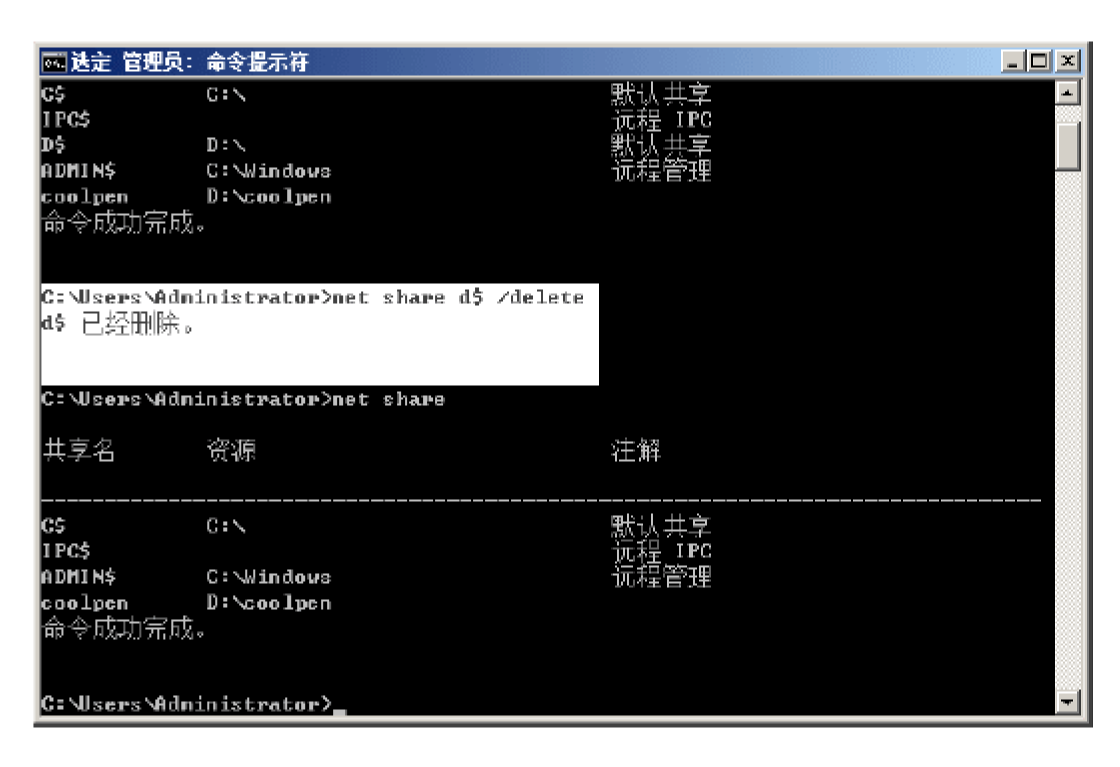


图 6-98 删除 D$默认共享

其中 D$表示系统默认共享 D 盘，其他如 C$、ADMIN$、IPC$等都可以使用此种格式删除。

在“/Delete”前必须要有空格。可以使用“NET SHARE ADMIN$”或“NET SHARE IPC$”建立“ADMIN$”或“NET SHARE IPC$”共享(如果共享存在，则为显示共享)，但需要注意的是，其他共享则不能使用该方法来建立默认共享。

如果需要删除所有的默认共享，可以使脚本命令(批处理文件方式)完成(即扩展名为“.bat”的文件)：

```
Net share IPC$ /delete
Net share Admin$ /delete
Net share C$ /delete
Net share D$ /delete
…
```

默认共享的盘符可以根据需要使用脚本命令分别删除，该批处理文件可以在命令提示符下运行，也可以将其添加到启动项中，如图 6-99 所示。这里创建一个名为“share.bat”的批处理文件，用以将系统的默认共享删除，并在命令提示符下运行。

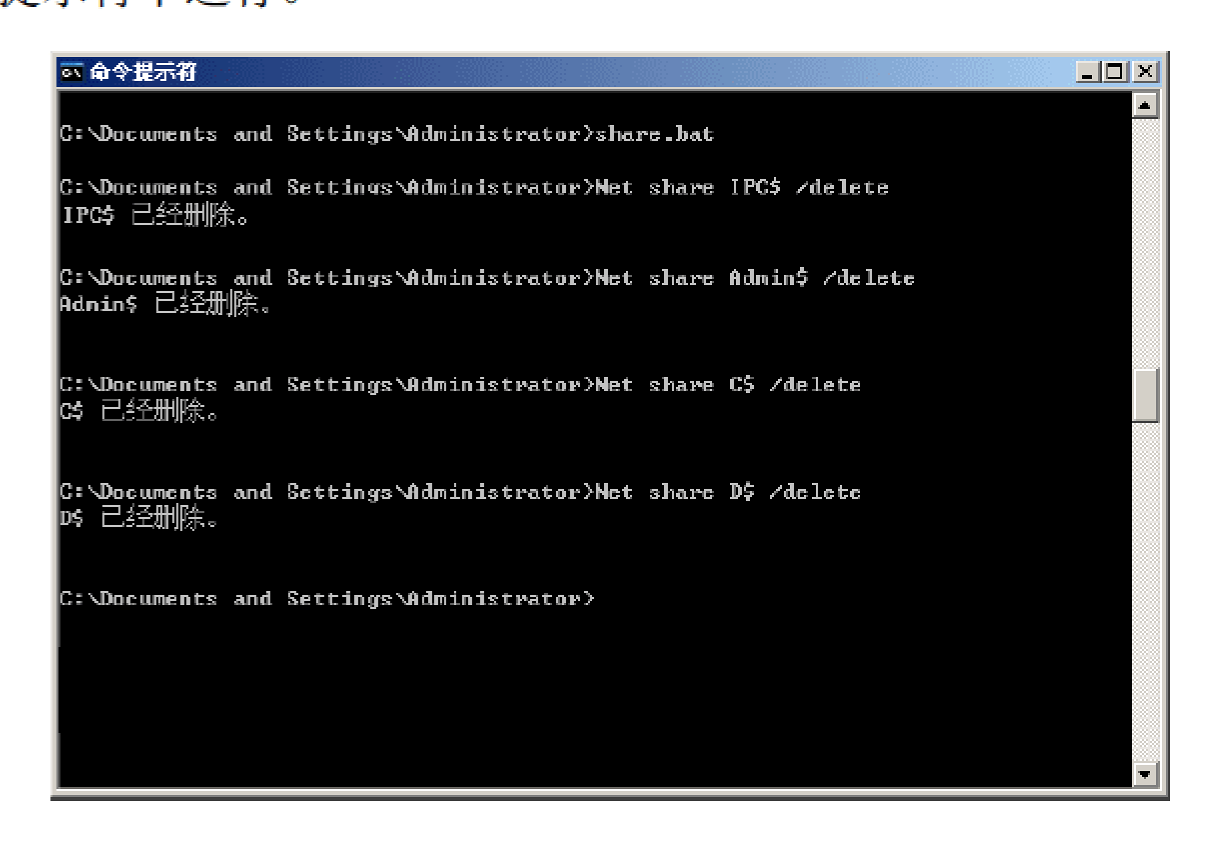


图 6-99　在命令提示符下运行批处理文件

(2) 关闭 Server 服务

默认共享使用的是计算机系统的 Server 服务，如果将该服务直接关闭，就可以直接删除默认共享。

① 依次选择“开始”→“管理工具”→“服务”选项，打开“服务”窗口，双击 Server 服务，打开“Server 的属性(本地计算机)”对话框，如图 6-100 所示。在“启动类型”下拉列表框中，选择“手动”，以免再次重新启动系统时服务随之启动。
② 单击“停止”按钮，显示如图 6-101 所示的“服务控制”对话框，开始停止 Server 服务。
③ 单击“确定”按钮，即可停止 Server 服务。再次打开命令提示符窗口，输入如下命令：

```
Net share
```

按 Enter 键，显示如图 6-102 所示的结果，提示 Server 服务没有启动，直接输入“n”并按 Enter 键即可。

使用这种方法停止默认共享后，其他共享也将同时被取消，应慎重选择。

(3) 修改注册表

使用前面两种方法停止完成系统默认共享，当系统重新启动后，默认共享会重新恢复。如果用户需要永久性地停止系统默认共享，可以通过修改注册表的方法来实现该目的。停止系统默认共享的键值，默认情况下在 Windows 操作系统上不存在，需要用户手动添加该键值，修改后重新启动计算机即可使该键值

生效。

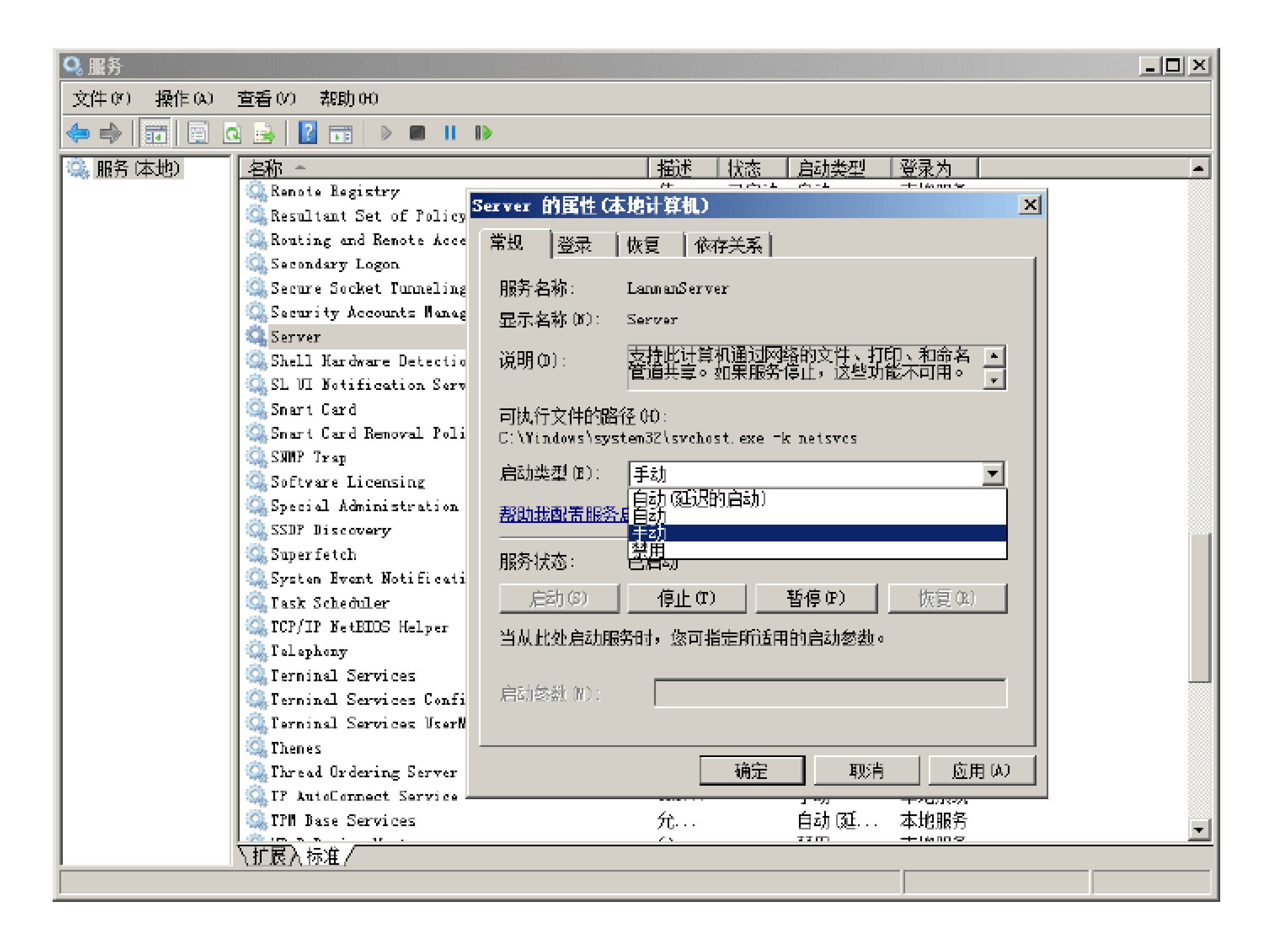
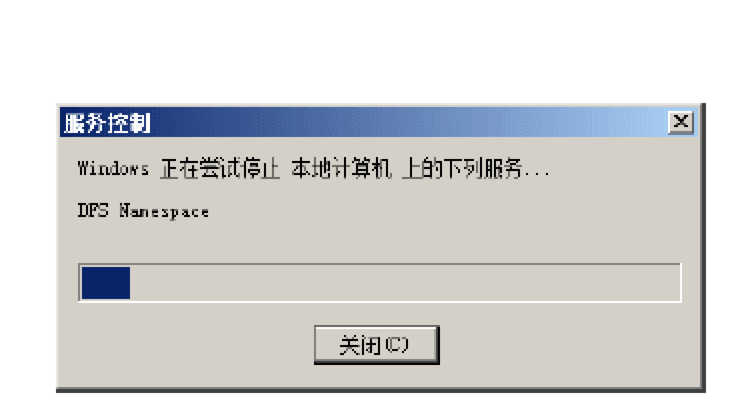


图 6-100　“Server 的属性(本地计算机)”对话框



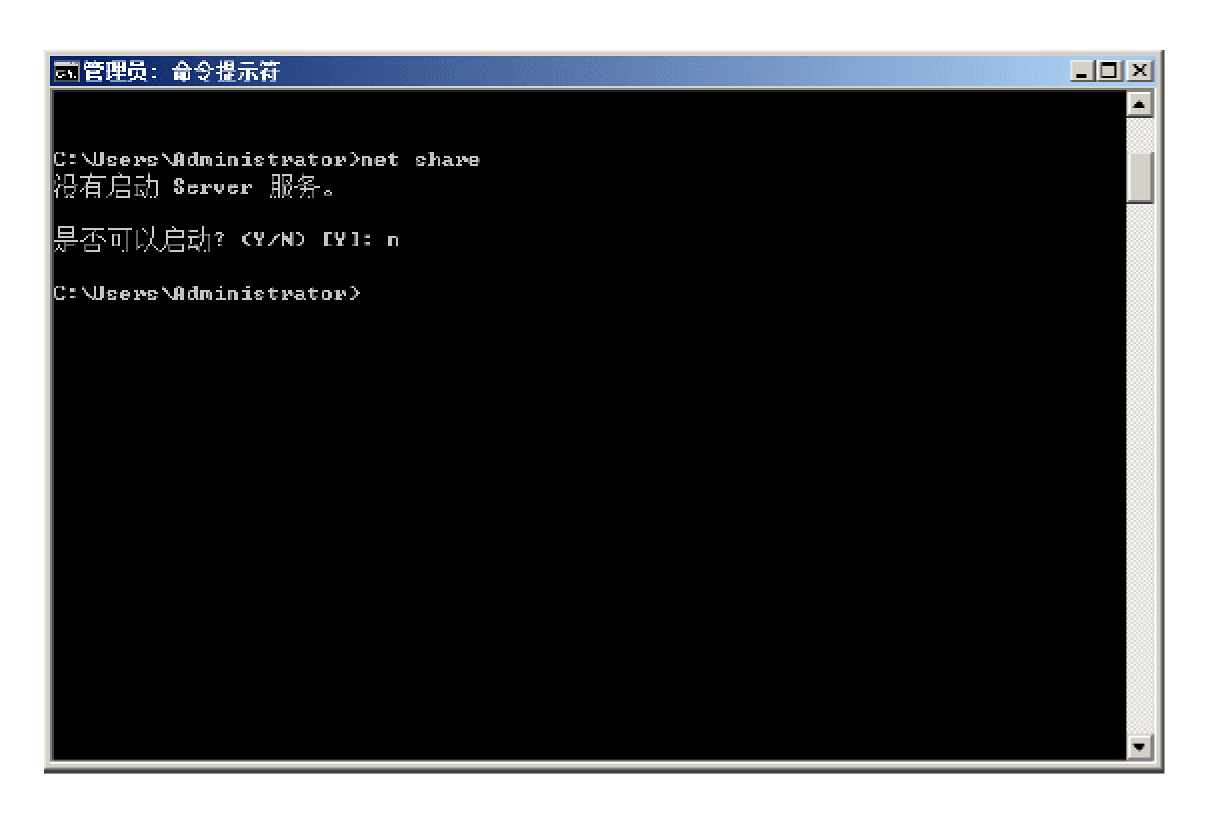


图 6-101　“服务控制”对话框　　　　图 6-102　关闭 Server 服务后

① 单击“开始”按钮，在“开始搜索”文本框中输入“regedit”并按 Enter 键，打开“注册表编辑器”窗口。依次展开如下注册表子项：[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\AutotunedParameters]，如图 6-103 所示。

② 在右侧的空白窗格中右击，在快捷菜单中选择“新建”命令，在子菜单中选择“Dword 值”选项，新建一个名为“AutoShareServer”的 Dword 值，并将其赋值为 00000000，如图 6-104 所示。

(4) Microsoft 网络的文件和打印机共享

除使用修改注册表的方法外，还可以使用卸载网卡相关属性的方法关闭默认共享。

① 在“控制面板”窗口中，打开如图 6-105 所示的“网络和共享中心”窗口。

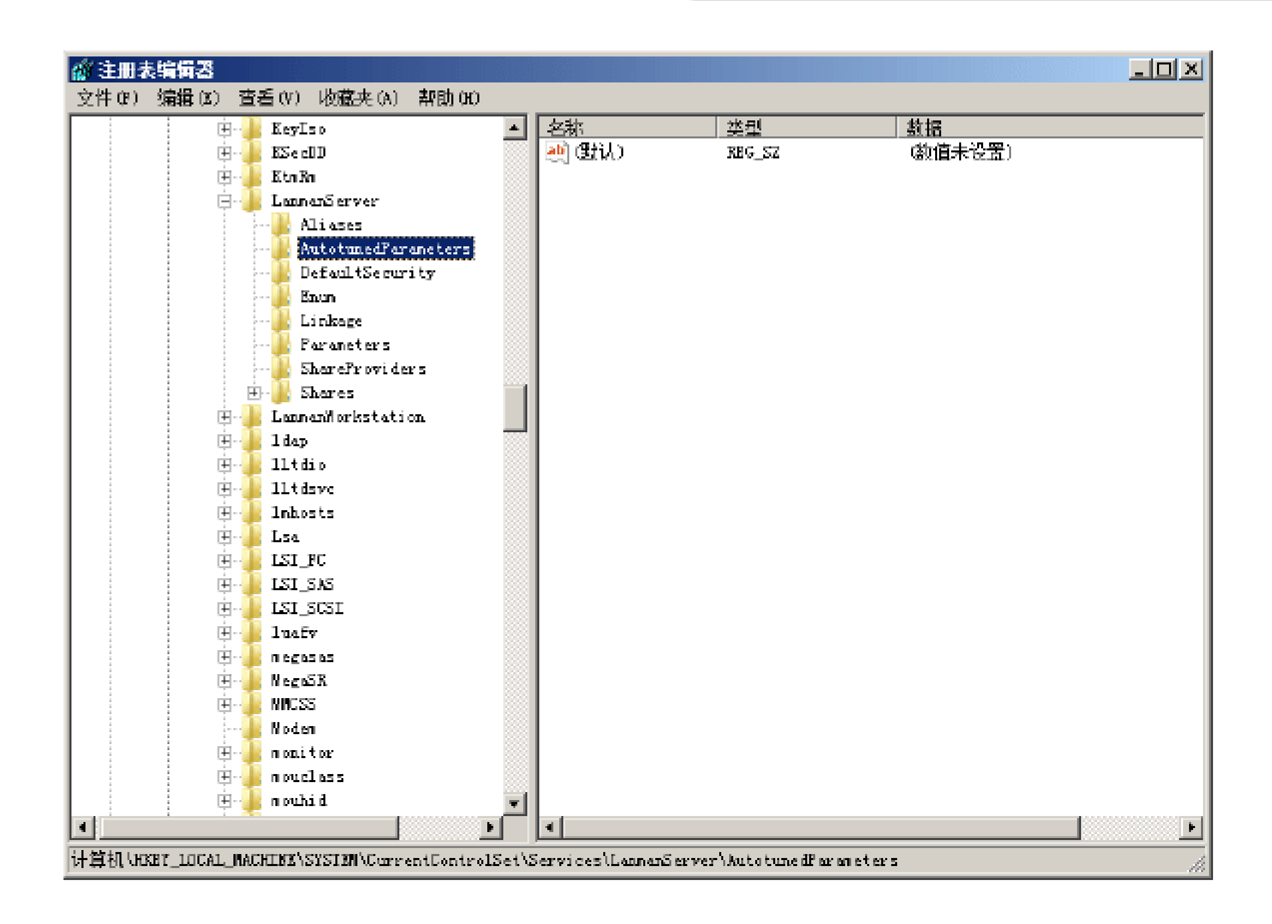


图 6-103　展开的注册表项目

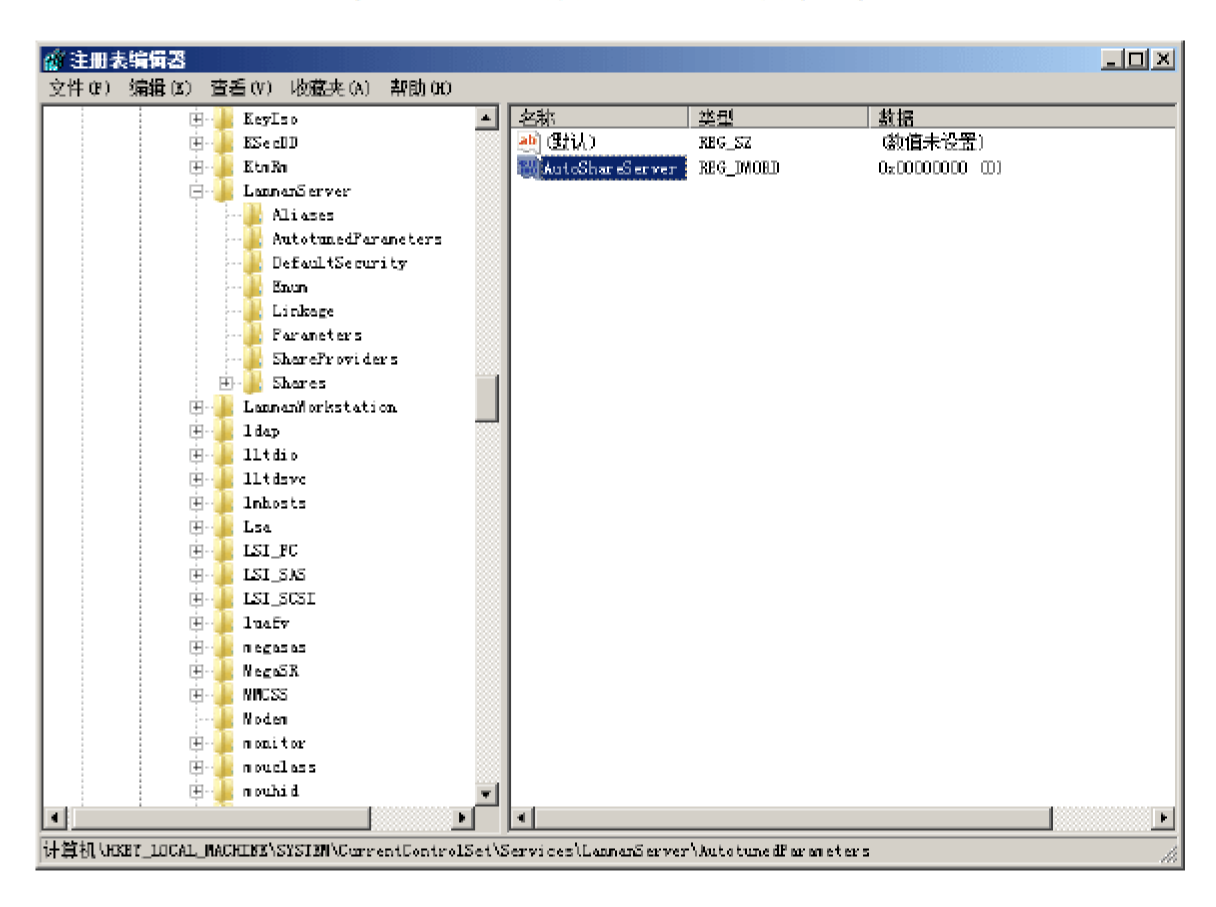


图 6-104　创建 DWORD 值



图 6-105　“网络和共享中心”窗口

② 单击“查看状态”链接，打开“本地连接 状态”对话框，单击“属性”按钮，显示如图 6-106

所示的“本地连接 属性”对话框。

③ 选中“Microsoft 网络的文件和打印机共享”复选框，单击“卸载”按钮，系统提示确认删除信息，显示如图 6-107 所示的“卸载 Microsoft 网络的文件和打印机共享”对话框。



图 6-106 “本地连接 属性”对话框

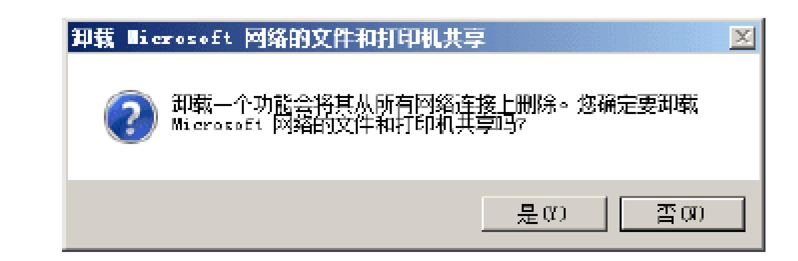


图 6-107 卸载信息提示

④ 单击“是”按钮，即可完成“Microsoft 网络的文件和打印机共享”项目的卸载。

第 7 章　网络服务安全

Windows Server 2008 是一款服务器操作系统，其设计初衷就是通过安装不同的服务组件，为网络提供各种服务。但因为其直接暴露于网络之下，所提供的网络服务的安全，将直接影响着提供服务的质量。微软在设计之初就想到多种可能遇到安全问题，因此，使用 Windows Server 2008 自身的不同安全措施可以进一步保证网络服务的安全。

关键词

- IIS 安全机制
- WWW 安全
- FTP 服务安全
- 终端服务安全
- 文件服务安全

7.1 IIS 安全机制

IIS 7.0 是 Windows Vista 和 Windows Server 2008 系统中的默认版本，相对于 IIS 6.0 而言，安全性和实用性都经过了重新设计和整合，模块化的管理特点更加清晰，管理员可以通过添加或删除相关功能模块来自定义服务器。IIS 7.0 支持多种安全机制，从管理控制台访问权限控制，到站点、目录的访问权限设置，从身份验证到传输加密，IIS 服务本身已经可以主动防御来自网络的攻击，同时配合 NTFS 权限的访问控制，可以大大提升服务器和站点的安全级别。

7.1.1 IIS 访问控制安全

通过为服务器配置适当的身份验证机制，可以确认任何请求访问网站的用户身份，以及授予访问站点公共区域的权限，同时还可以防止未经授权的用户访问专用文件和目录。除此之外，IIS 7.0 本身还提供了许多全新安全功能，如访问控制、IIS 管理器权限、授权规则等。

- .NET 信任级别。管理员可以通过此项安全设置为托管模块、管理程序和应用程序指定信任的级别，以提高网络组件和服务器的安全。该功能需要.NET 扩展组件的支持。
- IIS 管理器权限。该功能可以控制允许连接到网站或应用程序的用户对象，包括 IIS 管理器用户、Windows 用户或 Windows 组的成员。该功能仅适用于服务器连接。如果在 IIS 管理器中的服务器级别打开此功能，则可以查看被授予了 Web 服务器上所有网站和应用程序权限的用户，并且可以选择用户以删除该用户的网站或应用程序权限，提高服务器的安全性。
- IIS 管理器用户。通过该功能可以管理被允许连接到 Web 服务器上的网站或应用程序的用户账户。IIS 管理器凭据默认已经内置于 IIS 中，无法被 Windows 或服务器上的任何其他应用程序识别。
- 访问控制。与 IIS 6.0 中的“IP 地址和域名限制”功能类似，可以通过配置“允许”或“拒绝”访问服务器的 IP 地址或域名列表，实现对服务器的访问控制。
- ISAPI 和 CGI 限制。该功能可以指定，允许在 IIS 服务器上运行的 ISAPI 和 CGI 组件。CGI 是最常用的 Web 服务器功能的扩展，主要用于搭建动态网站环境。
- 服务器证书。证书可以用来建立安全套接字层(SSL)链接，也可以用于验证来访用户账户的身份。
- 功能权限委派。在 Windows Server 2008 中，管理员可以使用功能权限委派，为 WWW 服务器上的网站和应用程序配置 IIS 管理器功能的委派状态。从 IIS 管理器中配置功能的委派状态时，可以指定该功能在 IIS 7.0 的服务器级别配置文件中，是否处于锁定状态。如果某项功能被锁定，则只能从(向)服务器级别配置文件中，读取(写入)该功能的配置。但是，如果希望从(向)较低级别的配置文件(如网站或应用程序中的 Web.config 文件)中，读取(写入)配置时，则可以解除锁定。
- 管理服务。管理员可以使用功能配置 IIS 管理器的管理服务。利用管理服务，计算机和域管理员可以通过远程方式，管理 Web 服务器、站点和应用程序。
- 身份验证。IIS 7.0 可以提供 7 种身份验证方法，并且集成 Active Directory 服务的身份验证机制，如 AD 客户端身份验证、摘要式身份验证等，以及.NET 组件提供的 ASP.NET 模拟身份验证方法等。
- 授权规则。管理员通过为服务器配置相应的授权规则，可以指定授权用户访问网站或应用程序的规则。

7.1.2　NTFS 访问安全

NTFS 文件系统可以为数据提供安全和访问控制，可以限制用户和服务对文件和文件夹的访问。使用 NTFS 文件系统时，必须为用户账户授予相应的 NTFS 权限，该用户才能访问相应的文件或文件夹，否则就无法访问，从而在一定程度上保护了数据的安全。需要注意的是，NTFS 的安全性在本地计算机或网络中都是有效的。无论是以用户身份登录到服务器，还是通过网络访问共享文件夹，NTFS 安全性都有效。因此，从安全性角度考虑，应为 IIS 设置 NTFS 权限。

无论使用 IIS 搭建 Web 服务还是 FTP 服务，都应将文件存储在 NTFS 分区内，并利用 NTFS 权限来增强数据的安全性。在资源管理器中，右击 IIS 的安装目录(默认为%Systemroot%\Inetpub)选择快捷菜单中的“属性”选项，打开“inetpub 属性”对话框，切换到“安全”选项卡，单击“编辑”按钮，即可修改用户或组的访问权限，如图 7-1 所示。

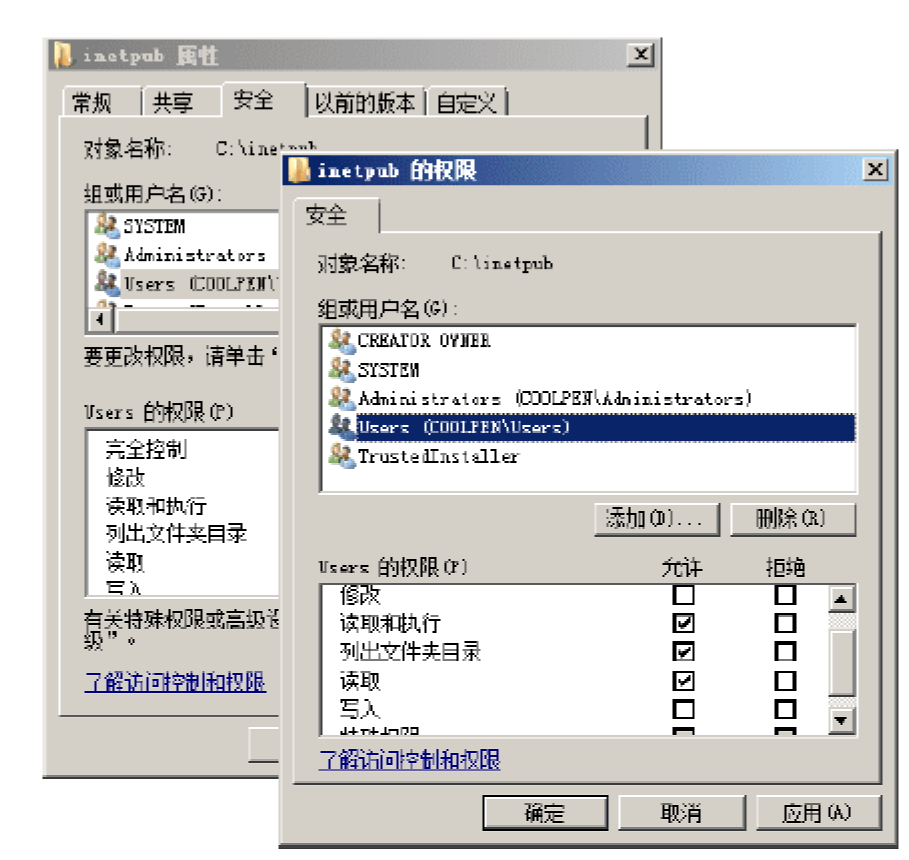


图 7-1　设置 NTFS 权限

如果 NTFS 的权限设置与 IIS 权限设置发生冲突，以最严格的设置为准。例如，NTFS 的权限设置为只读，而 IIS 权限设置为完全控制，那么，用户的访问权限将只能是“只读”。为了使服务器尽可能地安全，应该重新检查一下所有 IIS 文件夹的安全设置并进行适当的调整。

7.1.3　身份验证

在 IIS 7.0 中，支持以下 7 种身份验证方法，可以确认任何请求访问网站的用户身份以及授予访问站点公共区域的权限，同时又可防止未经授权的用户访问专用文件和目录。IIS 7.0 支持的身份验证方式如下：

- ASP.NET 模拟身份验证。启用该身份验证方式后，ASP.NET 应用程序可以在两种环境中运行，即作为通过 IIS 身份验证的用户或作为管理员设置的任意账户。该身份验证方式需要 ASP.NET 扩展组件的支持。
- Forms 身份验证。使用 Forms 身份验证，可以为公共服务器上的高流量网站或应用程序提供身份验证。该身份验证模式，可以使用户在应用程序级别管理客户端注册，而无需依赖操作系统提供的身份验证机制。
- 基本身份验证。基本验证会“模仿”一个本地用户(即实际登录到服务器的用户)，在访问 WWW 服务器时登录。因此，若欲以基本验证方式确认用户身份，用于基本验证的 Windows 用户，必须具有“本地登录”用户权限。默认情况下，主域控制器(PDC)中的用户账户，不授予“本地登录”用户的权限。使用基本身份验证方法，将导致密码以未加密形式在网络上传输。蓄意破坏系统安全的用户，可以在身份验证过程中使用协议分析程序，破译用户和密码。
- 摘要式身份验证。摘要式验证只能在域中使用。域控制器必须具有所用密码的纯文本副件，以便完成散列操作结果与浏览器发送散列值的比较。
- 匿名身份验证。这是 IIS 7.0 默认使用的身份验证方式，允许任何用户访问任何公共内容，而不用向客户端浏览器提供用户名和密码质询。如果某些内容只应当由选定用户查看，而且准备使用匿

名身份验证，则必须配置相应的 NTFS 文件系统权限，防止匿名用户访问这些内容。如果希望只允许注册用户查看选定的内容，则必须为这些内容配置适当的身份验证方法，如基本身份验证或摘要式身份验证。

- Windows 身份验证。集成 Windows 验证是一种安全的验证形式，需要用户输入用户账户和密码。用户名和密码在通过网络发送前会经过散列处理，因此可以确保安全性。当启用 Windows 验证时，用户的浏览器通过 WWW 服务器进行密码交换。Windows 身份验证使用 Kerberos v5 验证和 NTLM 验证。如果在 Windows 域控制器上安装了 Active Directory 服务，并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证，否则使用 NTLM 验证。
- 证书。可以用来建立安全套接字层(SSL)链接的数字凭据，也可以用于验证。

当不允许用户匿名访问时，还应当为 IIS 用户账户设置强密码，以实现 IIS 的访问安全。密码应该足够复杂且够长，可以通过使用数字、符号和英文字母(包括大小写)结合的方式来设置密码，长度一般在 6 位以上，并且通过经常修改密码，封锁失败的登录尝试，以及设定账户的有效期等方法对一般用户账户进行管理。

如果 IIS 服务器在域环境中运行，则还将安装一种仅适用于域环境的身份验证方式，即“Active Directory 客户证书身份验证”。允许用户使用 Active Directory 目录服务功能，将用户映射至客户证书，以便进行身份验证。将用户映射至客户证书可以自动验证用户的身份，而无需使用基本、摘要式或集成 Windows 身份验证等其他身份验证方法。

7.1.4 IIS 安装安全

在安装 IIS 时应注意以下问题：

- 选择非域控制器作为 IIS 服务器。安装 IIS 过程中，系统将自动创建“IUSR_计算机名”匿名账户，如果所选服务器是域控制器，则该用户账户将被添加到域用户组中(Users)，从而把应用于组的访问权限，提供给访问 IIS 服务器的每个匿名用户，这不仅给 IIS 带来潜在危险，而且还可能威胁整个网络的安全。
- 选择非系统分区作为安装目录。把 IIS 安装在非系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户侵入系统分区，所以在安装 IIS 的 Web、FTP 等服务时，应尽量避免将 IIS 服务器安装在非系统分区上。
- 安装在 NTFS 类型分区上。相对于 FAT32 分区而言，NTFS 分区拥有较高的安全性和可管理性，并且磁盘利用效率高，可以设置复杂的访问权限，以适应不同信息服务的需求。
- 只安装必需的组件。除非特别需要，否则，不要安装 Internet 打印以及 ASP.NET、CGI 等动态网站扩展组件，以避免恶意用户借助相应的组件漏洞或设置错误，实现对 IIS 服务器的攻击。
- 定制自己需要的安全功能组件。IIS 7.0 提供的更为丰富的安全功能设置，管理员可以根据 IIS 服务器的需求定制适当的安全限制。

7.2 WWW 安全

WWW 服务是常用网络服务之一，通过 IIS 可以搭建信息发布、信息查询、电子商务、电子政务等各种用途的 Web 网站。此外，许多基于 Web 管理界面的其他网络服务，同样需要用到 WWW 服务器的安全，

如邮件服务器、流媒体服务器等。因此，WWW 服务器的安全性，将影响到本地系统，甚至整个网络的安全性，必须通过相应的安全机制控制来访用户的访问。

7.2.1　用户控制安全

WWW 服务器的主要功能就是为用户提供信息发布和查询平台，信息的面向对象不同，所以就需要对访问用户进行控制，通过设置适当的身份验证方式即可实现。例如，如果信息面向所有用户，则可以使用匿名身份验证；如果仅面向部分用户，则可以仅赋予这些用户对信息的访问权限。配置身份验证可以确保服务器的安全，同时还可以为来访用户提供身份验证并生成服务器日志。

① 依次选择“开始”→“管理工具”→“Internet 信息服务(IIS)管理器”选项，打开“Internet 信息服务(IIS)管理器”窗口，依次展开“LIUXH(服务器名称)”→“网站”→“Default Web Site(默认 Web 站点)”，在中间窗格中选择“身份验证”图标，如图 7-2 所示。

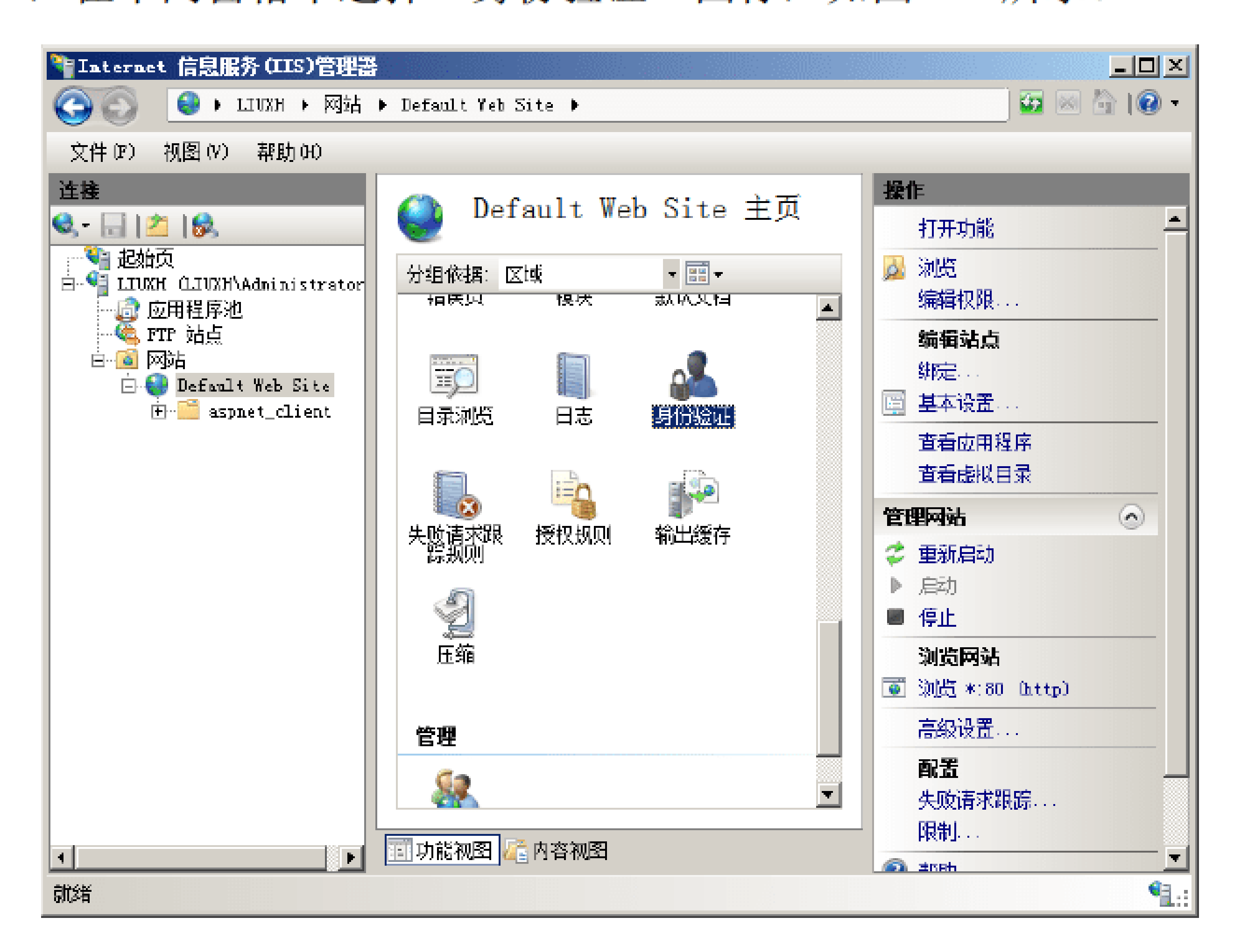


图 7-2　“Internet 信息服务(IIS)管理器”窗口



提示：在“分组依据”下拉列表框中，可以选择适当的分类条件，包括类别、区域和不进行分组几种。所选分类条件的不同，布局也会有所不同。

② 在“操作”栏中单击“打开功能”链接，或者直接双击“身份验证”，显示如图 7-3 所示的“身份验证”窗口。



提示：如果采用默认方式安装 Windows Server 2008 中的 IIS 7.0，将只安装必须的“匿名身份验证”组件，管理员也可以在安装过程中，根据需要选择希望安装的组件，或者在安装完成后，再次添加希望使用的身份验证安全组件，如图 7-4 所示。

③ 在“身份验证”窗口中，选择“匿名身份验证”并单击“操作”栏中的“编辑”链接，显示如图 7-5 所示的“编辑匿名身份验证凭据”对话框。默认选择“特定用户”单选按钮，IIS 7.0 默认使用安装过程中自动创建的 IUSR，作为用户名进行匿名访问。如果选择“应用程序池标识”单选按钮，则可以允许 IIS 进程，使用在应用程序池的属性页上指定的账户运行。

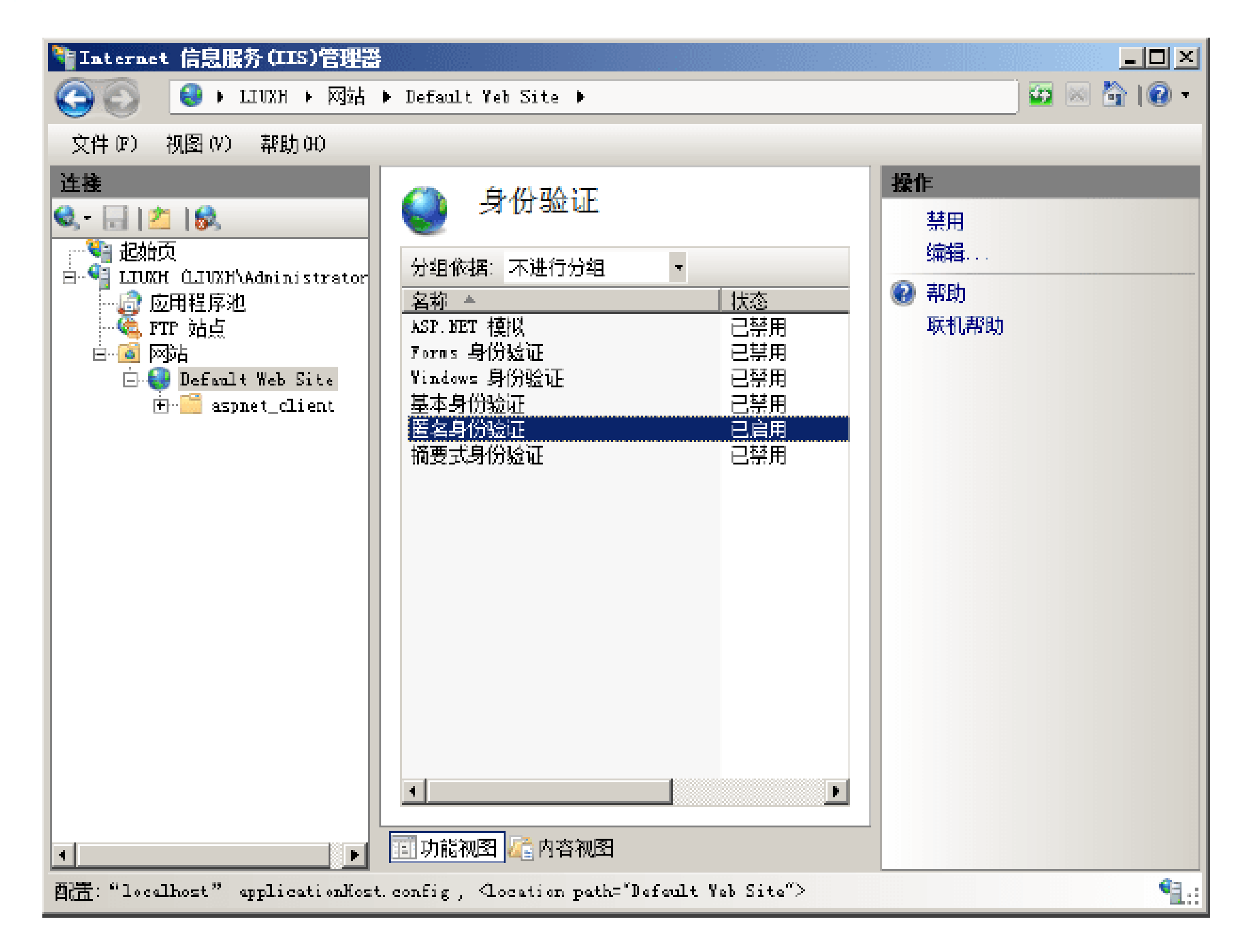


图 7-3 “身份验证”窗口

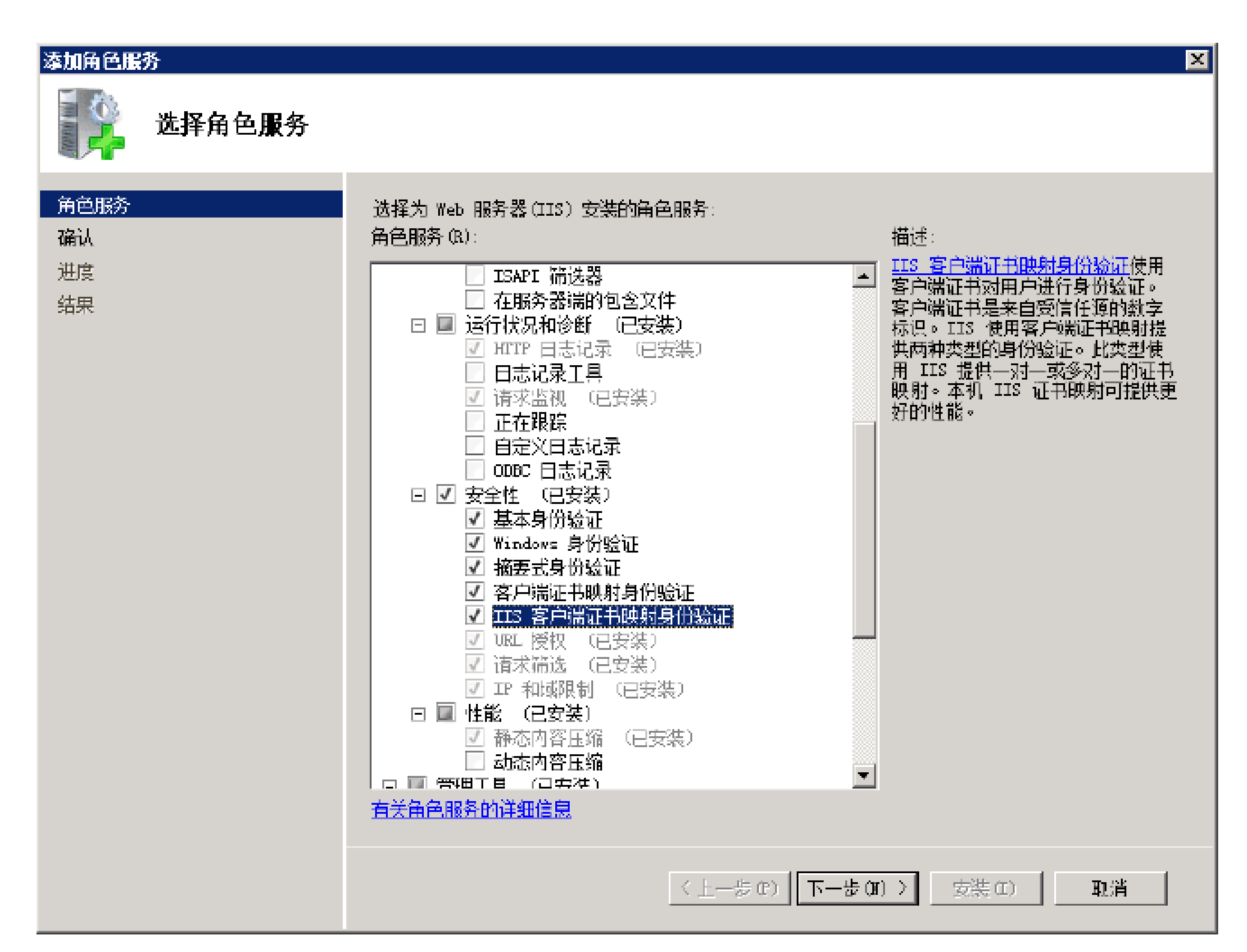




图 7-4 添加功能组件

图 7-5 “编辑匿名身份验证凭据”对话框

④ 单击“设置”按钮，显示如图 7-6 所示的“设置凭据”对话框。输入用户名、密码后单击“确定”按钮，替换系统默认的 IUSR 账户，再次单击“确定”按钮，保存设置。

⑤ 更改系统默认匿名访问账户，虽然可以起到一定的安全保护作用，但仍不能适用于安全需求较高的 Web 服务器。在“身份验证”窗口中，选择“匿名身份验证”选项，单击“操作”栏中的“禁用”链接，即可禁用匿名访问。此时，来访用户必须使用有效的用户账户凭证，通过 Web 服务器的身份验证，才可以进行正常访问。在“身份验证”窗口中，选择希望使用的身份验证方式，单击“操作”栏中的“启用”链接即可。

⑥ 选择“基本身份验证”方式，在“操作”栏中单击“编辑”链接，显示如图 7-7 所示的“编辑基本身份验证设置”对话框。在“默认域”文本框中，输入默认情况下对用户进行身份验证时所依据的域名，如 coolpen.net。在“领域”文本框中，输入将使用已通过默认域身份验证凭据的 DNS

域名或地址，可以选择为基本身份验证提供“领域”，如 liuxh.coolpen.net。




图 7-6 “设置凭据”对话框



图 7-7 “编辑基本身份验证设置”对话框


提示：如果在“领域”框中，输入默认域名，则在用户名和密码质询期间，内部的 Microsoft Windows 域名可能会暴露给外部用户。

⑦ 单击“确定”按钮，保存设置即可。同时还可以启用多种身份验证方式。

7.2.2 访问权限控制

通过设置适当的访问权限，可以严格控制来访用户对于指定类型的文件的访问。管理员可以根据实际情况，为特殊文件类型设置访问策略，指定授予 IIS 中的 Web 服务器、网站、应用程序、目录或文件级别的处理程序的功能权限类型。

1. 编辑功能权限

通过配置功能权限可以设置访问策略，访问策略指定 IIS 中所有处理程序可以具有的权限类型。可以在访问策略中启用或禁用的功能权限包括读取、脚本和执行。处理程序能否运行由访问策略以及处理程序所需的访问设置共同决定。如果处理程序需要未在访问策略中启用的功能权限类型，该处理程序将被禁用，并且该处理程序(基于处理程序映射)处理的所有请求都将失败，除非请求可以由另一个处理程序处理。

① 在 IIS 7.0 管理控制台中，单击欲配置的服务器、站点或目录，在主页窗口中双击“处理程序映射”图标，显示如图 7-8 所示的“处理程序映射”窗口。“已启用”列表中显示的是当前站点支持的文件类型。

② 右击需要设置的文件类型(以 ASPClassic 为例)，选择快捷菜单中的“编辑功能权限”命令，打开如图 7-9 所示的“编辑功能权限”对话框。各权限的描述如下：

- 读取。选中“读取”复选框，可以启用需要对虚拟目录具有读取访问权限的处理程序。如果要提供静态内容，或者要配置默认的文档和目录浏览，则应当在访问策略中启用读取权限。默认情况下，读取权限处于启用状态。
- 脚本。选中“脚本”复选框，可以启用需要对虚拟目录具有脚本权限的处理程序。
- 执行。选中“执行”复选框，以启用需要对虚拟目录具有执行权限的处理程序。只有当“脚本”复选框处于选中状态时，才会启用“执行”复选框。只有当希望除了脚本之外还允许运行可执行文件(如 .exe、.dll 和 .com 文件)时，才应当在访问策略中启用执行权限。

出于安全和性能方面的考虑，应当只对已经过测试且应用程序需要的程序启用执行权限。

③ 单击“确定”按钮，保存设置。



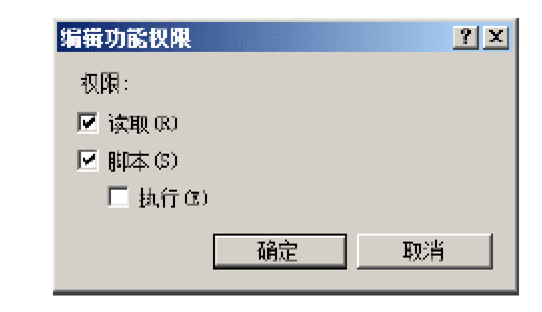


图 7-8 “处理程序映射”窗口　　图 7-9 “编辑功能权限”对话框

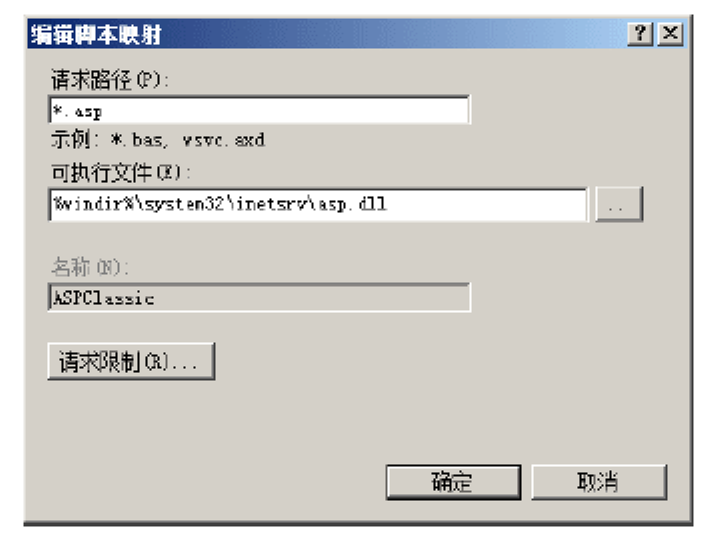
2. 设置请求限制

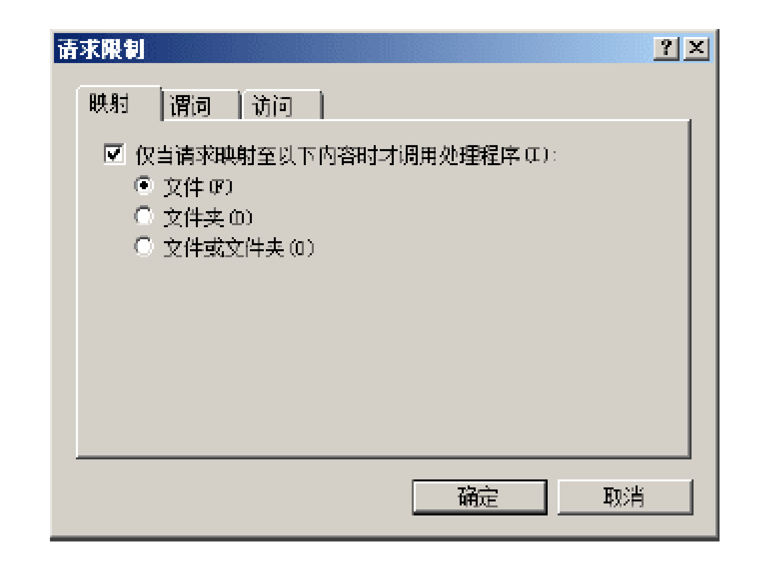
如果希望处理程序只响应对特定资源类型的请求(例如文件或文件夹，或者对特定谓词的请求)，则可以为处理程序映射配置可选限制，也可以指定处理程序需要具有何种访问权限才能在虚拟目录中运行。处理程序所需的访问权限设置以及“处理程序映射”功能的访问策略，共同决定了处理程序能否运行。

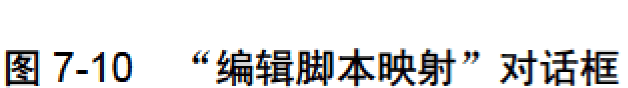
① 在“处理程序映射”窗口中，双击希望设置请求限制的应用程序名称(以 ASPClassic 为例)，打开如图 7-10 所示的“编辑脚本映射”对话框。

② 单击“请求限制”按钮，打开“请求限制”对话框，默认显示如图 7-11 所示的“映射”选项卡。如果希望处理程序仅响应针对特定资源类型的请求，则可以选中“仅当请求映射至以下内容时才调用处理程序”复选框，并选择以下选项：

- “文件”，用于使处理程序仅在所请求的目标资源是文件时才做出响应。
- “文件夹”，用于使处理程序仅在所请求的目标资源是文件夹时才做出响应。
- “文件或文件夹”，用于使处理程序仅在所请求的目标资源是文件或文件夹时才做出响应。






图 7-10 “编辑脚本映射”对话框　　图 7-11 “映射”选项卡

③ 切换至如图 7-12 所示的“谓词”选项卡，可以选择以下选项：

- “全部谓词”，如果选择此选项，则不论请求中发送的谓词如何，处理程序均对请求做出响应。
- “下列谓词之一”，如果选择此选项，则处理程序将响应包含特定谓词的请求。然后，请在对应

的框中输入一个或多个谓词。

④　切换至如图 7-13 所示的“访问”选项卡，可以选择下列选项：

- “无”，如果选择此选项，即使在未启用任何访问策略选项的情况下，处理程序也将运行。
- “读取”，如果选择此选项，则处理程序会在访问策略中启用了“读取”的情况下运行。
- “写入”，如果选择此选项，则处理程序会在访问策略中启用了“写入”的情况下运行。
- “脚本”，如果选择此选项，则处理程序会在访问策略中启用了“脚本”的情况下运行。这是默认选项。
- “执行”，如果选择此选项，则处理程序会在访问策略中启用了“执行”的情况下运行。



图 7-12　“谓词”选项卡

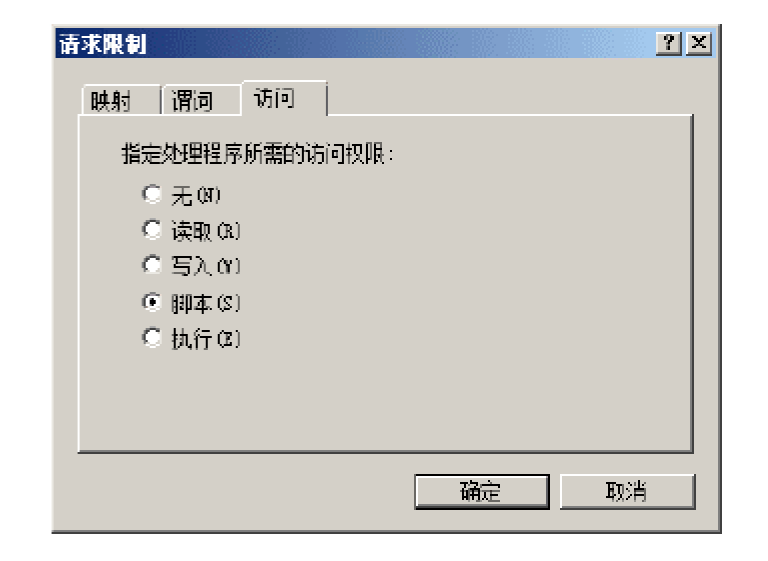


图 7-13　“访问”选项卡

请确保处理程序所需的访问权限设置正确无误，否则处理程序将可能在无意中运行。例如，如果为 ISAPI-dll 处理程序将处理程序所需的访问权限从“执行”更改为“读取”，那么，即使在功能的访问策略中仅启用了“读取”，ISAPI 扩展也将能够运行。

⑤　单击“确定”按钮，保存设置。

7.2.3　授权规则

通过配置 Web 站点的授权规则，可以指定允许授权用户访问网站和应用程序的规则，例如允许或拒绝指定用户或组访问网站等。这种授权规则，可以是基于用户账户或组的，也可以是基于应用程序角色的。

①　在“Internet 信息服务(IIS)管理器”的“Default Web Site 主页”窗口中，双击“授权规则”图标，显示如图 7-14 所示的“授权规则”窗口，系统默认已经创建了一条允许所有用户访问该站点的规则。

②　在“操作”栏中单击“添加拒绝规则”链接，显示如图 7-15 所示的“添加拒绝授权规则”对话框，选择“所有匿名用户”单选按钮，拒绝所有匿名用户对该站点的访问。选中“将此规则应用于特定谓词”复选框，还可以设置相关描述信息，如“拒绝所有匿名用户访问”。



提示：如果选择“指定的角色或用户组”或“指定的用户”单选按钮，则需要在对应文本框中，输入对应的组名称或用户账户名称。

③　单击“确定”按钮，即可将新建规则添加到“授权规则”列表中，如图 7-16 所示。管理员也可以直接选择默认授权规则，单击“编辑”链接，来生成自己需要的新规则。添加允许授权规则的方法与此完全相同，此处不再赘述。

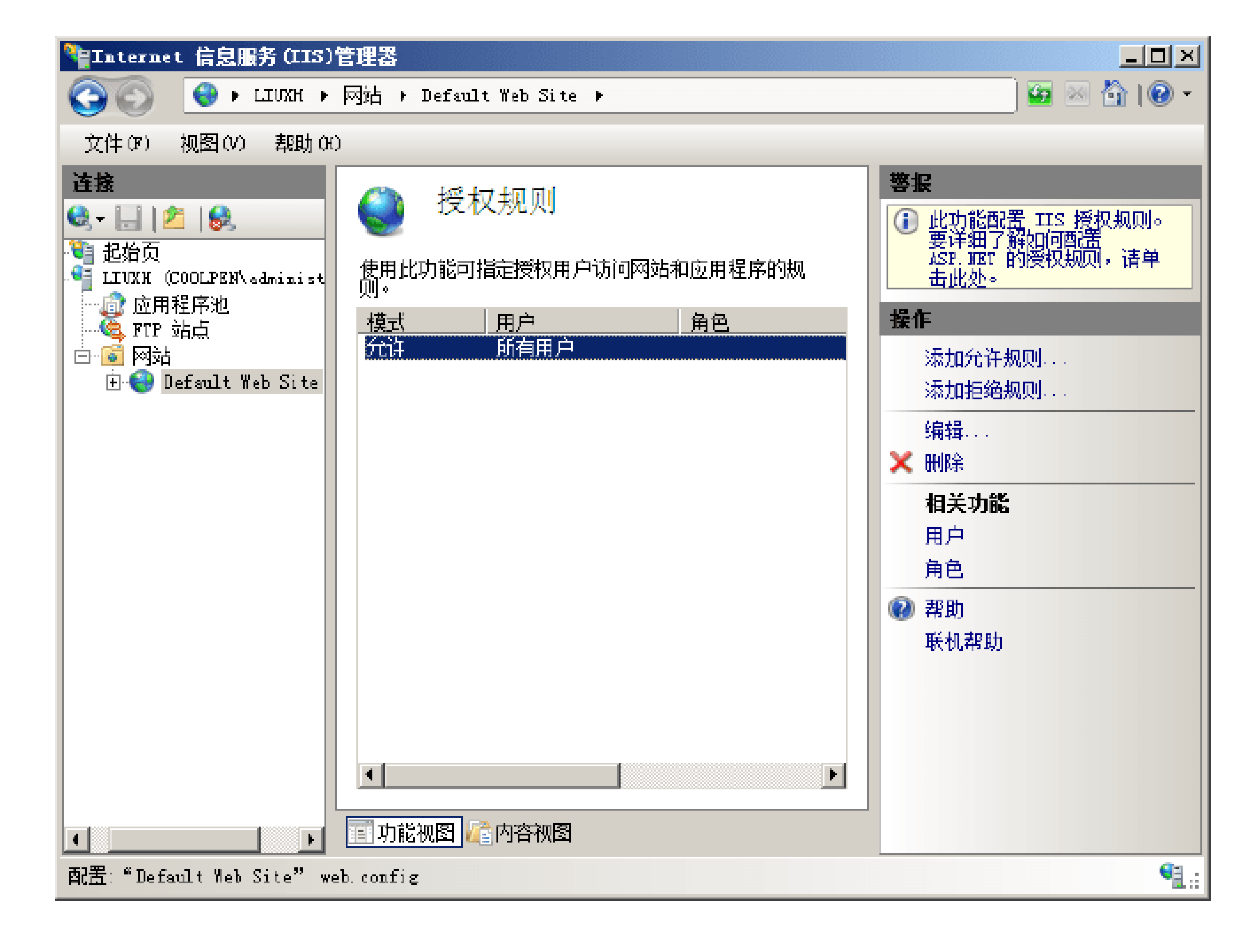


图 7-14 “授权规则”窗口

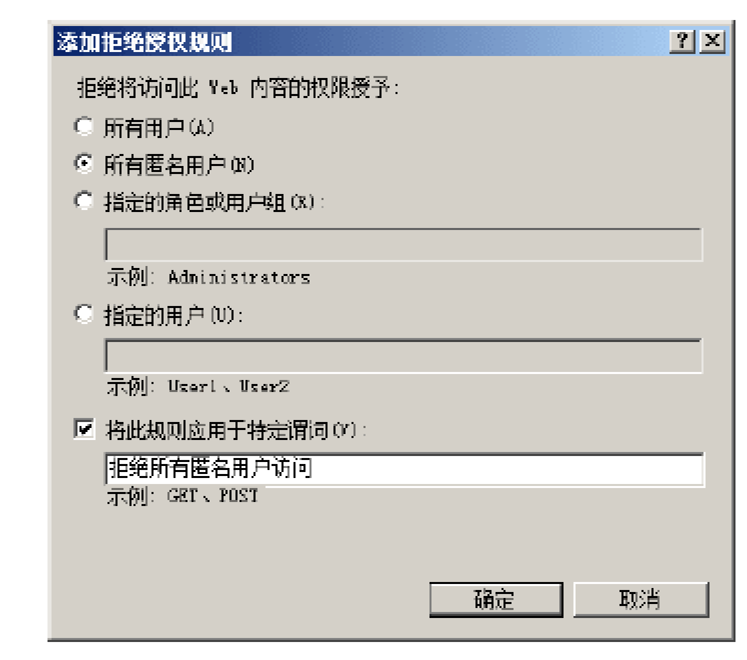


图 7-15 “添加拒绝授权规则”对话框

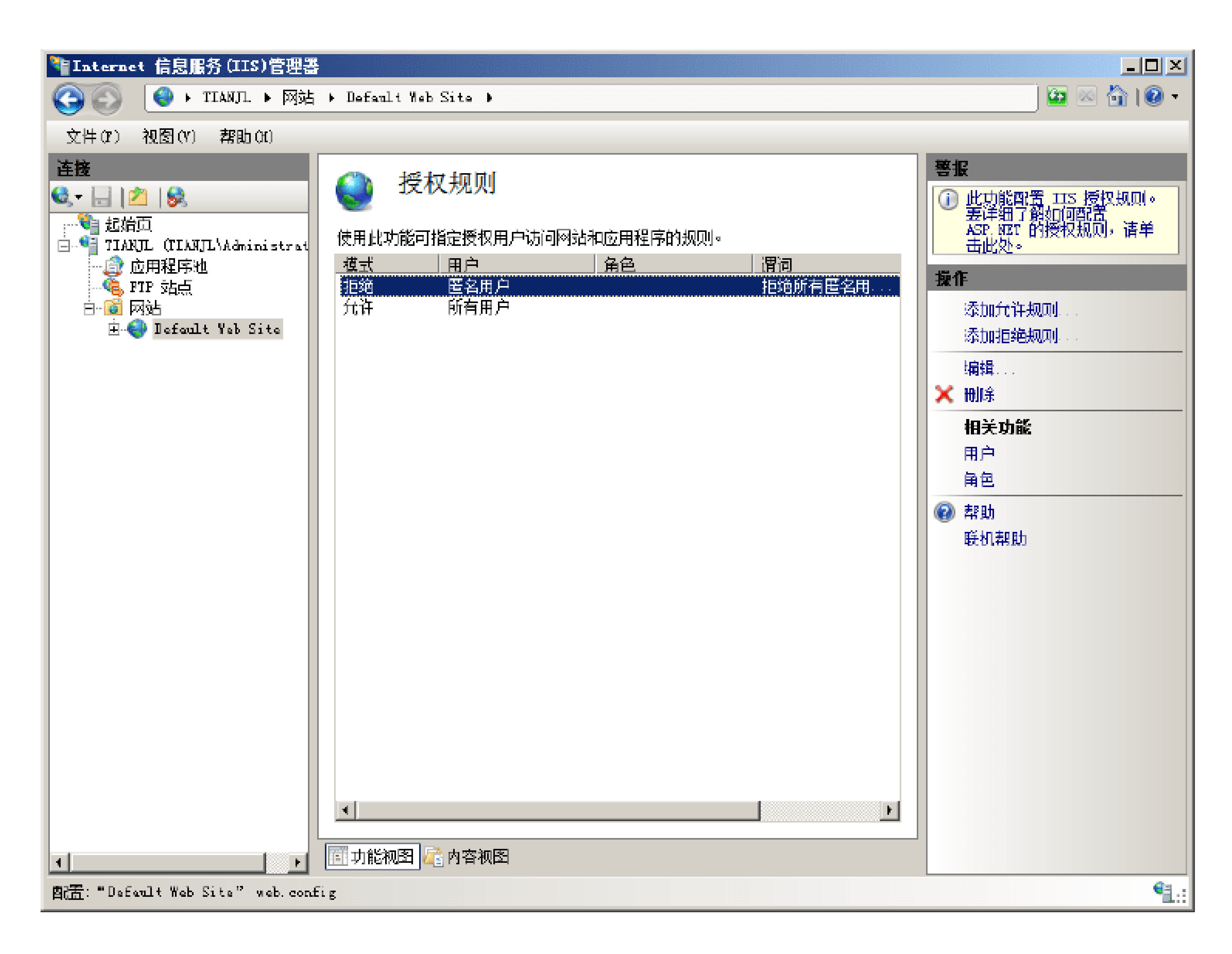


图 7-16 创建成功的授权规则

注意：如果某个角色、用户或组已经被某条规则明确拒绝了访问权限，则不能由另一条规则授予访问权限。另外，当配置基于.net 应用程序角色和.net 用户账户的授权规则时，需要借助 SQL Server 2005/2008 方可实现。

7.2.4 IPv4 地址控制

默认情况下，IIS 会自动检查每个来访者的 IP 地址，通过 IP 地址的访问来防止或允许某些特定的计算

机、域，甚至整个网络访问站点。因此，通过 IP 地址限制的方法在 Internet 上排除未知用户是非常有效的。同时，IIS 7.0 还提供了基于 Windows 域的访问限制，管理员可以禁止或允许来自指定域的用户，访问站点或目录，该功能默认是未启用的。

① 在“Internet 信息服务(IIS)管理器”的“Default Web Site 主页”窗口中，双击“IPv4 地址和域限制”图标，显示如图 7-17 所示的“IPv4 地址和域限制”窗口。

② 单击“添加允许条目”链接，打开“添加允许限制规则”对话框。系统默认选择“特定 IPv4 地址”单选按钮，在对应文本框中，输入想要允许访问的单个 IP 地址即可。建议选择“IPv4 地址范围”单选按钮，并输入相应的主机 IP 地址和“掩码”，如图 7-18 所示，可以同时添加多个被允许访问的主机 IP 地址。



图 7-17　“IPv4 地址和域限制”窗口

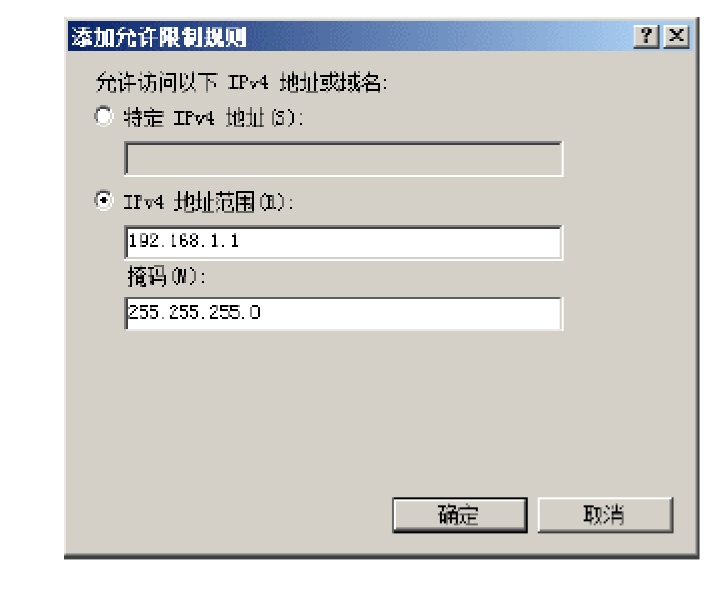


图 7-18　“添加允许限制规则”对话框

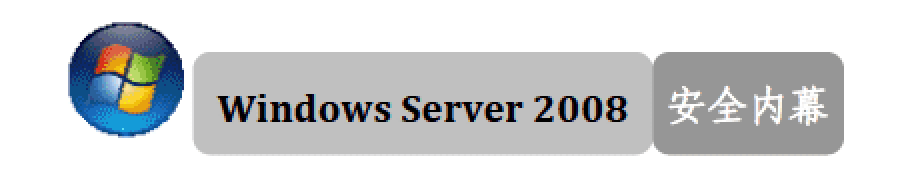
③ 单击“确定”按钮，新创建的限制规则即可被添加到“IPv4 地址和域限制”列表中。“添加拒绝条目”的操作步骤与之类似，此处不再赘述。

④ 在“操作”栏中单击“编辑功能设置”链接，显示如图 7-19 所示的“编辑 IP 和域限制设置”对话框，用户还可以根据域名来限制要访问的计算机。在“未指定的客户端的访问权”下拉列表框中，设置除指定的 IP 地址外的客户端，访问该网站时进行操作，用户可以根据需要在下拉列表框中，选择“允许”或“拒绝”选项。若选中“启用域名限制”复选框，即可启用域名限制。需要注意的是，通过域名限制访问会要求 DNS 反向查找每一个连接，这将会严重影响服务器的性能，建议不要使用。

⑤ 在“操作”栏中单击“恢复为继承的项”链接，显示如图 7-20 所示的“IPv4 地址和域限制”对话框，恢复功能以从父配置中继承设置，该操作将为当前功能删除本地配置设置(包括列表中的项目)，应慎重使用。

图 7-19　“编辑 IP 和域限制设置”对话框

⑥ 在“操作”栏中单击“查看经过排序的列表”链接，显示如图 7-21 所示的窗口。IIS 7.0 是按照限制规则列表中条目的顺序依次执行的。例如，当前规则列表中包括两条限制条目：拒绝 IP 地址为 192.168.1.21 的主机访问，允许整个 192.168.1.1 ～ 192.168.1.254 网段访问，即被拒绝的 IP 地址 192.168.1.21 又在被允许访问的网段内。此时，如果经过排序后拒绝在先，则将拒绝指定用户访问；如果允许在



先则将允许该用户访问。

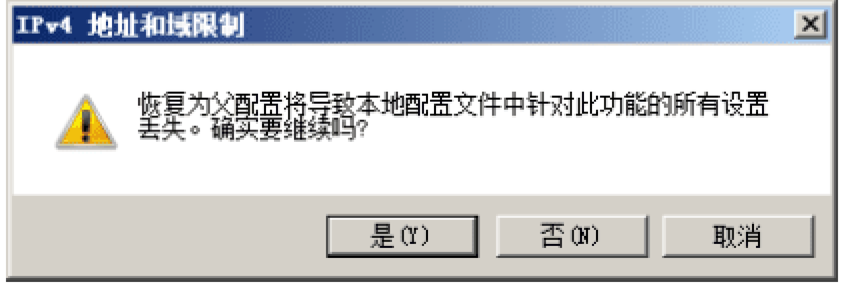


图 7-20 “IPv4 地址和域限制”对话框



图 7-21 查看经过排序的列表

⑦ 在经过排序的限制列表中，选择想要移动的限制条目，单击“上移”或“下移”链接，即可调整执行顺序。

7.2.5 IP 转发安全

IIS 服务可提供 IP 数据包的转发功能，此时，充当路由器角色的 IIS 服务器将会把从 Internet 接口收到的 IP 数据包转发到内部网中。在此。为了提高 IIS 服务的安全性，应当禁用 IP 转发功能。

要设置 TCP/IP 转发需要编辑注册表。需要注意的是，修改注册表有一定的危险性，如果编辑不当就会造成系统故障，因此，应事先备份注册表。

运行 Regedit.exe 命令打开注册表编辑器，展开注册表项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\，在右侧窗口中找到 IPEnableRouter 项，双击打开，如果其数值为 1，此时应改为 0，如图 7-22 所示。单击“确定”按钮，关闭注册表编辑器即可。

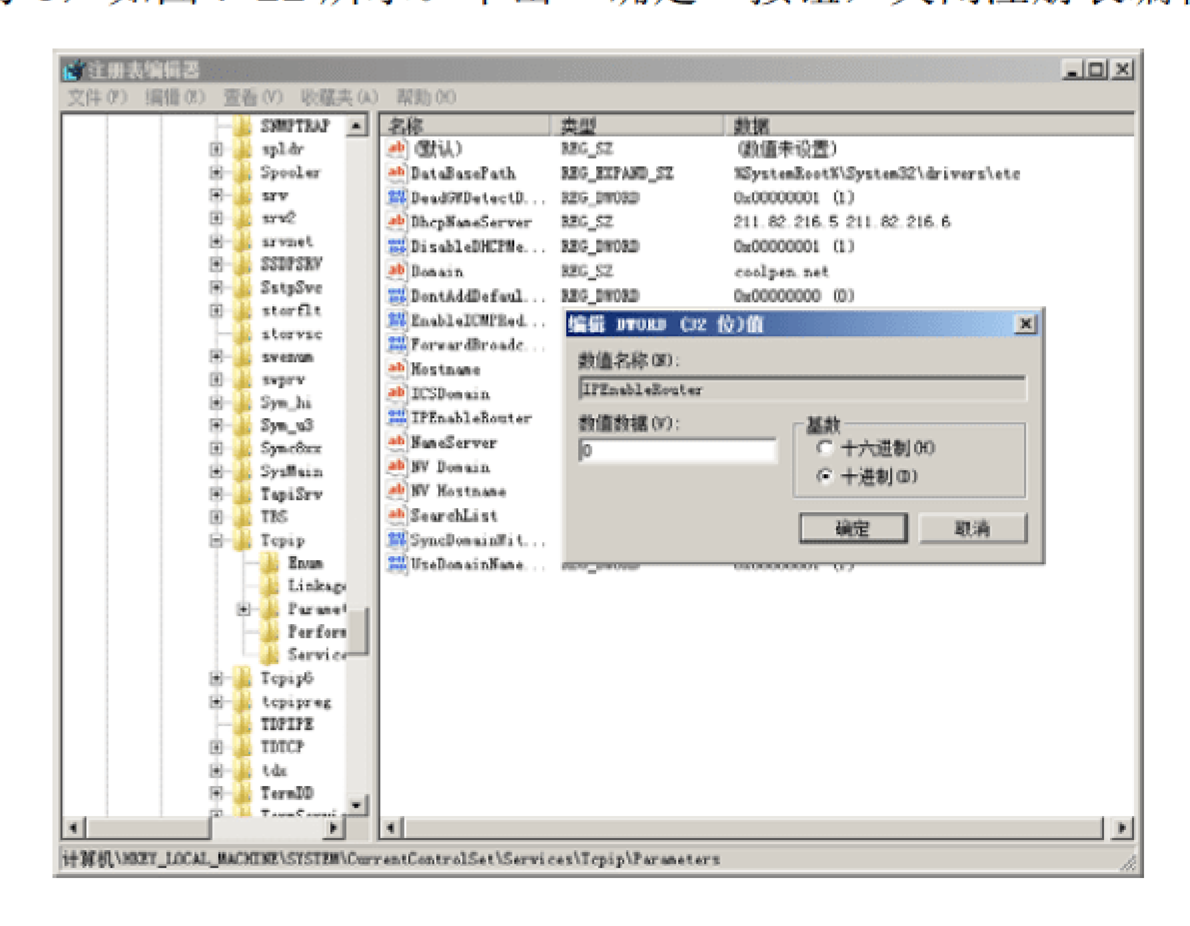


图 7-22 禁用 IP 转发安全

7.2.6　SSL 安全

SSL 安全功能可以通过对传输信息进行加密，实现 Web 客户端与 Web 服务端的安全传输，避免数据被中途截获和篡改。对于安全性要求很高的、可交互性的 Web 网站，建议采用 SSL 加密方式。若欲实现 SSL 通讯，Web 服务器必须拥有有效的服务器证书。

1. Web 服务器端设置

要想为站点启用 SSL 安全保护，必须在服务器端创建用于 SSL 加密的证书和启用 SSL 设置。

(1) 创建服务器证书

"服务器证书"包含关于服务器的信息，服务器允许客户在共享敏感信息之前，对其加以积极识别，WWW 服务器只有安装有效服务器证书后，才拥有安全通信功能。

① 在"Internet 信息服务(IIS)管理器"窗口中，选择希望使用 SSL 安全加密的站点，双击"服务器证书"图标，显示如图 7-23 所示的"服务器证书"窗格。安装 IIS 7.0 过程中，系统已经自动创建了一个服务器证书，管理员可以直接应用该证书，也可以导入已有证书，或者创建新的证书。这里选择"创建自签名证书"，各项操作功能含义如下：

- 导入。还原已丢失或损坏、但之前已备份的服务器证书，也可以应用来自其他用户或证书颁发机构的证书。
- 创建证书申请。如果网络存在第三方证书颁发机构(CA，即证书服务器)，可以通过这种方法向证书服务器提交证书申请，通过审核后即可获得属于自己的服务器证书。
- 完成证书申请。安装从证书颁发机构接收到的证书，并开始应用。
- 创建域证书。向内部证书颁发机构提供有关当前服务器的信息。
- 创建自签名证书。创建仅在服务器测试环境中使用、并且可用于排除第三方证书故障的证书，无需向第三方服务器提交和等待批准。
- 查看。查看所选证书的详细信息。
- 导出。导出所选证书的备份，可以继续应用于其他目标服务器，或保存为备份，以便重新安装服务器或证书损坏后，可以快速导入。
- 删除。删除选择的证书。

② 在右侧"操作"栏中，单击"创建自签名证书"链接，显示如图 7-24 所示的"创建自签名证书"对话框。在"为证书指定一个好记的名称"文本框中，输入服务器证书的文件名。

③ 单击"确定"按钮，创建自签名证书完成，新创建的证书即可显示在列表中，选中创建成功的自签名服务器证书"safe_site"，单击"查看"链接，显示如图 7-25 所示的"证书"对话框。在这里可以查看该证书的名称、颁发者、颁发给、到期日期和证书哈希等详细信息。

④ 在"Internet 信息服务(IIS)管理器"窗口的"网站"列表中，右击希望应用此证书的站点(注意，必须是 https 站点)，选择快捷菜单中的"编辑绑定"选项，显示如图 7-26 所示的"网站绑定"对话框。

⑤ 选中 https 站点并单击"编辑"按钮，显示如图 7-27 所示的"编辑网站绑定"对话框，"IP 地址"和"端口"设置保持默认即可。在"SSL 证书"下拉列表中，选择刚刚创建的自签名证书 safe_site。

⑥ 单击"确定"按钮，返回"网站绑定"对话框。单击"关闭"按钮保存设置并退出。

(2) 启用 SSL 设置

在"Internet 信息服务(IIS)管理器"窗口中，如图 7-28 所示单击需要启用 SSL 设置的站点，并在主窗

口中双击“SSL 设置”图标，显示如图 7-28 所示的“SSL 设置”窗格。



图 7-23 “服务器证书”窗格

图 7-24 “创建自签名证书”对话框

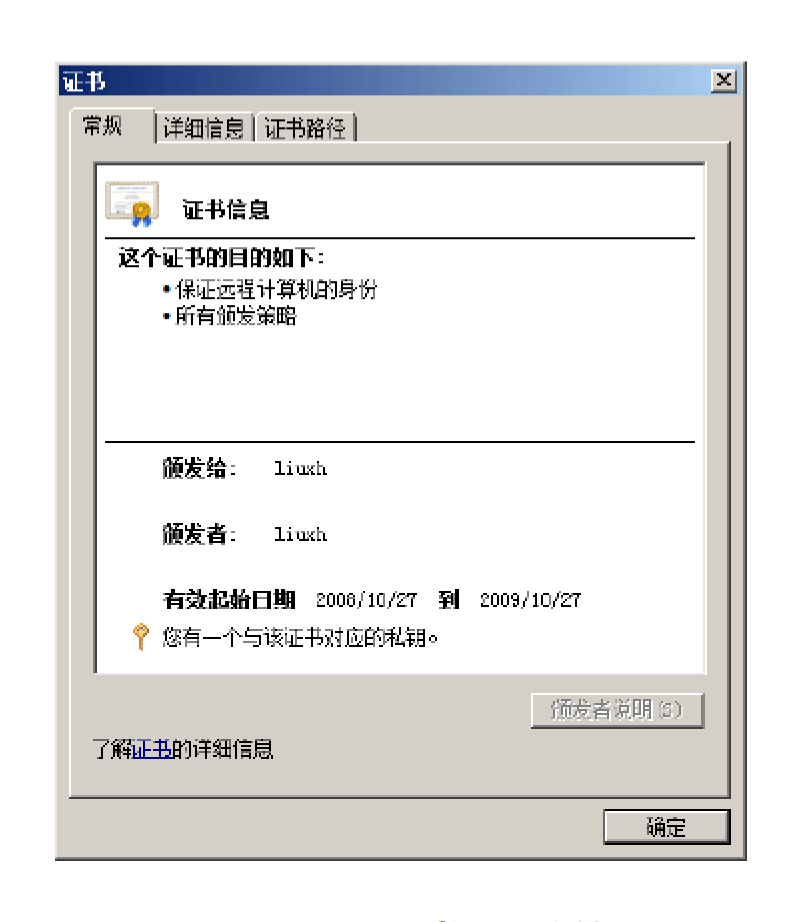


图 7-25 “证书”对话框

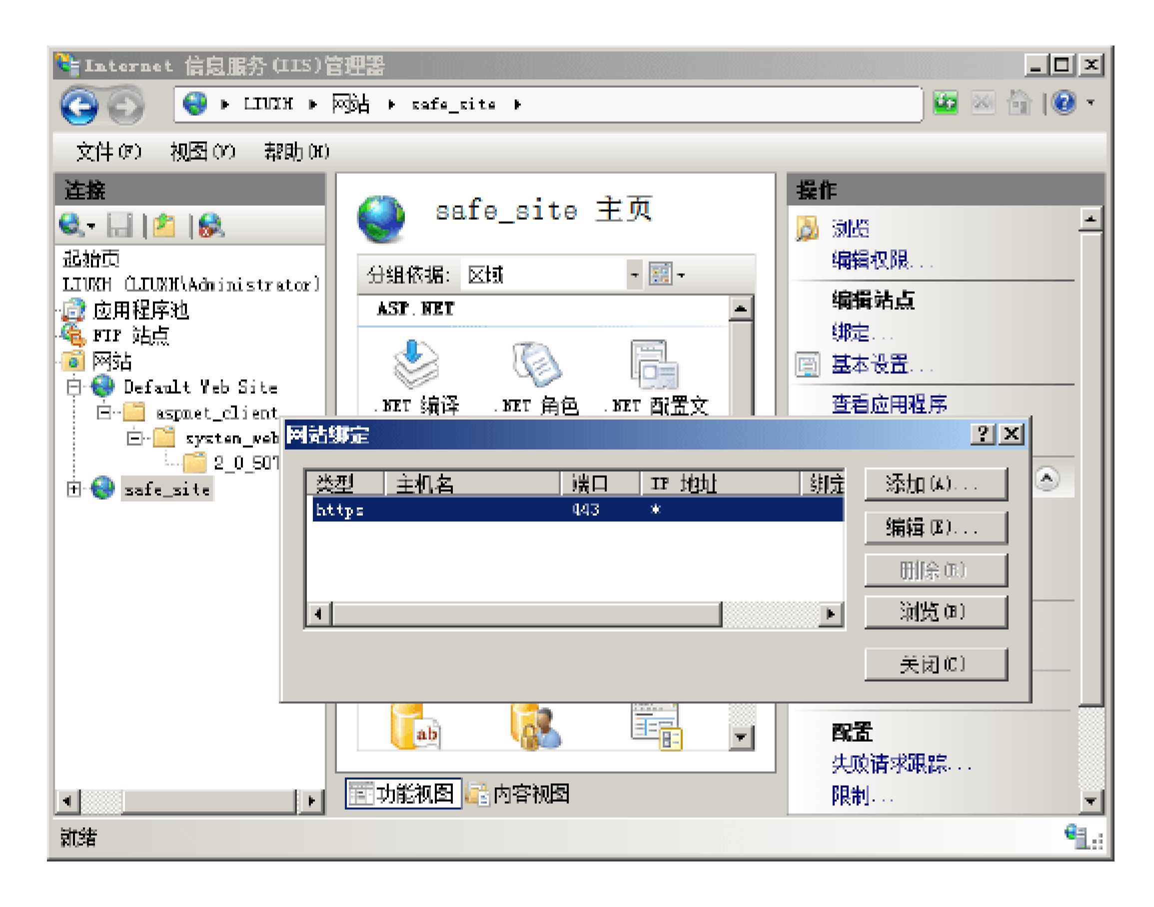


图 7-26 “网站绑定”对话框

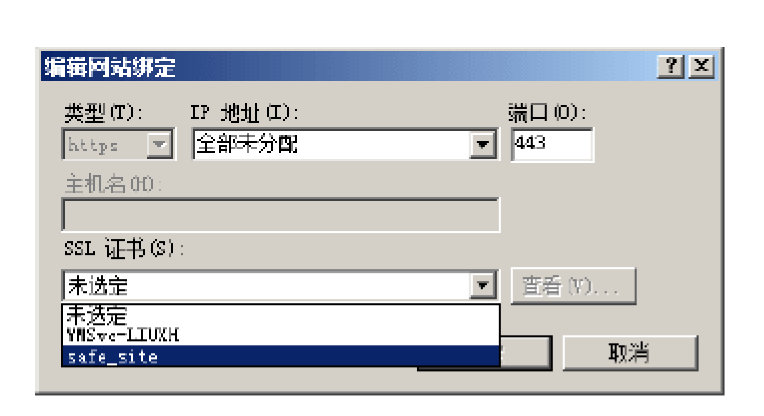


图 7-27 “编辑网站绑定”对话框

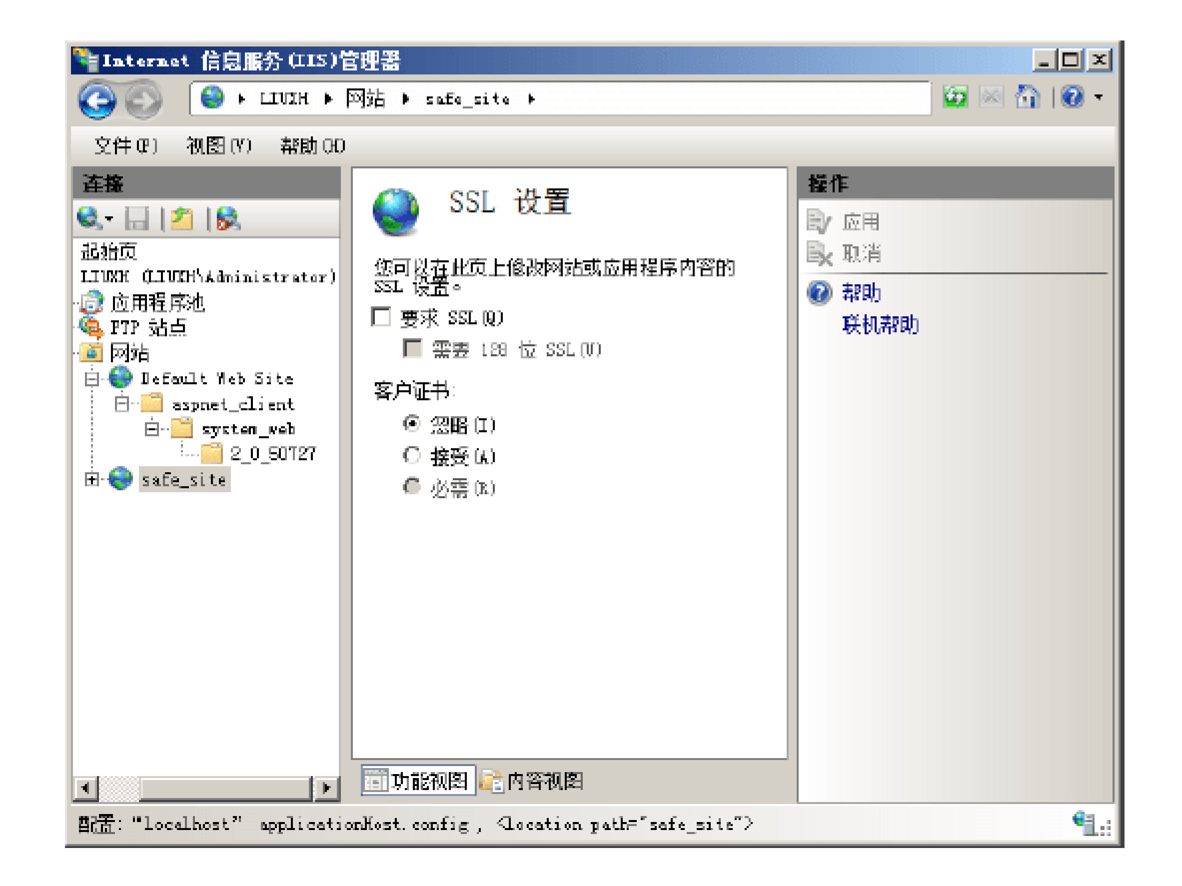


图 7-28 “SSL 设置”窗格

选中“要求 SSL”复选框，以启用 40 位数据加密方法，该方法可以用来帮助确保服务器与客户端之间传输的安全性。该选项设置既可用于 Intranet 环境，也可用于 Internet 环境。如果选中“需要 128 位 SSL”，则安全性更高，不过传输加密数据所需的带宽也将随之增加。

在“客户证书”选项框中选择“接受”单选按钮，即可启用服务器端的 SSL 设置，接受客户端证书(若提供)，在允许客户端获得内容访问权限之前验证客户端身份。系统默认选择“忽略”单选按钮，即如果提供客户端证书，则该设置不会接受，因此该设置的安全性最低。如果选择“必要”单选按钮，则在接受用户访问之前要求提供对应证书，验证客户端身份的有效性。

设置完成后，在“操作”栏中单击“应用”链接即可应用设置。

2. 客户端设置

用户访问使用 SSL 协议加密的站点或网页，与访问普通站点略有不同。首先，使用加密传输的站点使用 https://开头的 URL；其次，用户必须连接到站点指定的证书服务器，获取相关数字证书并安装。

7.2.7　审核 IIS 日志记录

服务器上的每个 Web 站点，运行过程中都会产生相应的日志信息，用于记录服务器的运行情况、客户端访问情况等。IIS 日志数据可以记录用户对站点内容的访问，确定哪些内容比较受欢迎，还可以记录有哪些用户非法入侵网站、确定计划安全要求和排除潜在的网站问题等。使用 IIS 的日志功能，可以配置 IIS 在 Web 服务器上记录请求的方式。

① 在“Internet 信息服务(IIS)管理器”窗口的站点(以 Default Web Site 站点为例)主页中，双击“日志”图标，显示如图 7-29 所示的“日志”窗格。系统默认状态是为每个站点创建一个日志文件，管理员可以在服务器配置主页的“日志”窗格中，将其修改为：为每服务器创建一个日志文件。

② 在“日志文件”选项框的“格式”下拉列表中，选择“W3C”选项，IIS 7.0 可以提供 4 种日志文件格式：

- W3C。W3C 扩展日志文件格式，是一个包含多个不同属性、可自定义的 ASCII 格式，可以记录重要的属性，并通过省略不需要的属性字段来限制日志文件的大小。各属性字段以空格分开，时间以 UTC 形式记录。
- NCSA。NCSA 是美国国家超级计算技术应用中心公用格式，是一种固定的(不能自定义的)ASCII 格式，记录了关于用户请求的基本信息，如远程主机名、用户名、日期、时间、请求类型、HTTP 状态码和服务器发送的字节数。项目之间用空格分开，时间记录为本地时间。
- IIS。IIS 日志文件格式是固定的(不能自定义的)ASCII 格式。IIS 格式比 NCSA 公用格式记录的信息多。IIS 格式包括一些基本项目，如用户的 IP 地址、用户名、请求日期和时间、服务状态码和接收的字节数。另外，IIS 格式还包括详细的项目，如所用时间、发送的字节数、动作(例如，GET 命令执行的下载)和目标文件。这些项目用逗号分开，使得格式比使用空格作为分隔符的其他 ASCII 格式更易于阅读。时间记录为本地时间。
- 自定义。将 IIS 配置为对自定义的日志记录模块使用自定义格式。如果选择此选项，则“日志”页将被禁用，因为无法在 IIS 管理器中配置自定义日志。

③ 单击“选择字段”按钮，显示如图 7-30 所示的“W3C 日志记录字段”对话框，用户根据实际需要进行设置即可。

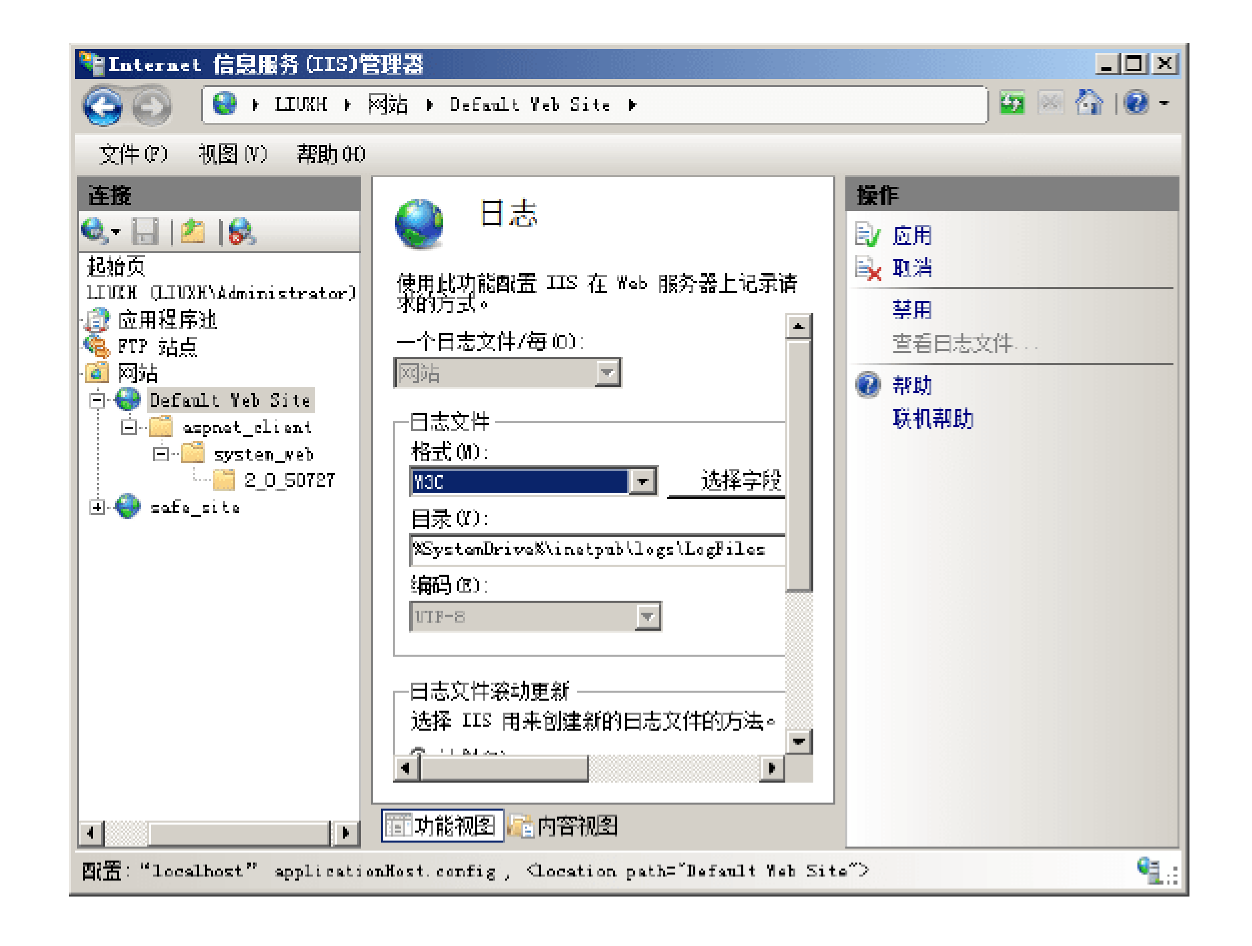


图 7-29 “日志”窗格

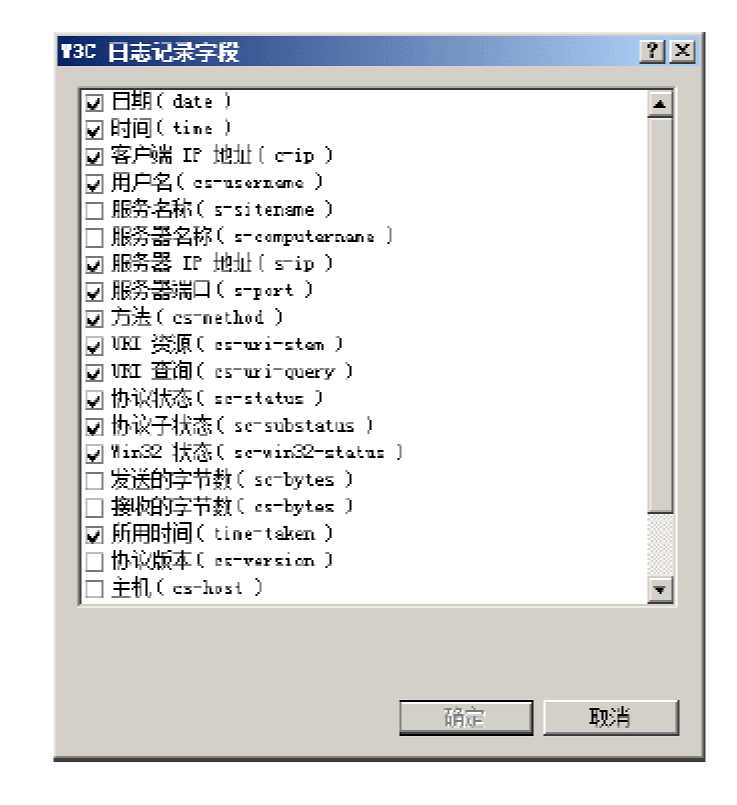


图 7-30 “W3C 日志记录字段”对话框

④ 在“目录”文本框中，单击“浏览”按钮，设置日志文件的保存位置，默认保存目录为：%SystemDrive%\inetpub\logs\LogFiles。

⑤ 在“日志文件滚动更新”选项框中，设置创建新日志文件的方式。包括：

■ 计划。可以固定的时间更新日志，例如每天更新。

■ 最大文件大小。当日志文件达到该大小时，自动更新日志文件。

■ 不创建新的日志文件。将所有的网站日志记录全部记录到单个文件中。

⑥ 在 Windows Server 2008 系统中，管理员可以通过“事件查看器”，管理和查看 Web 服务器和站点日志，如图 7-31 所示。

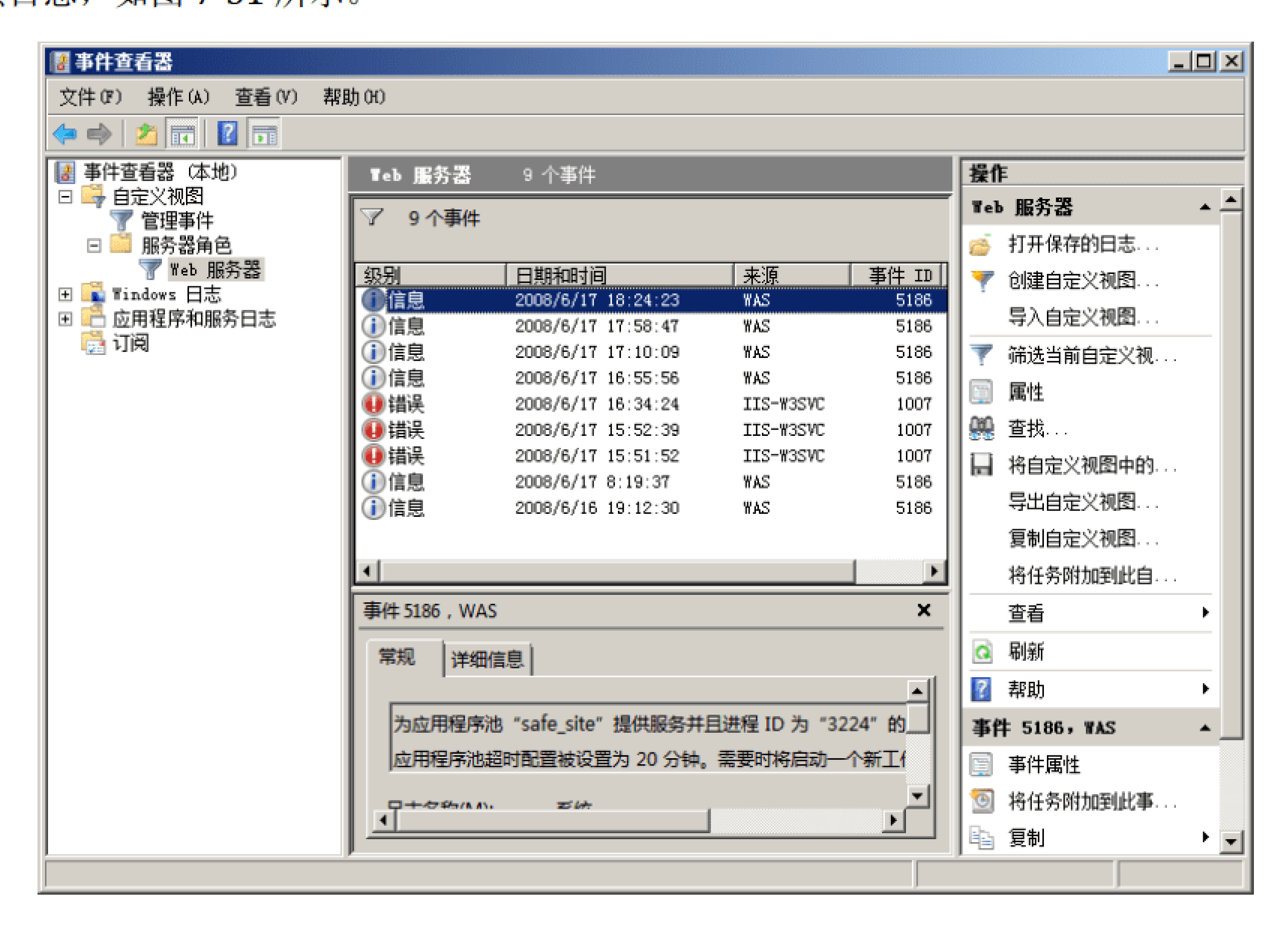
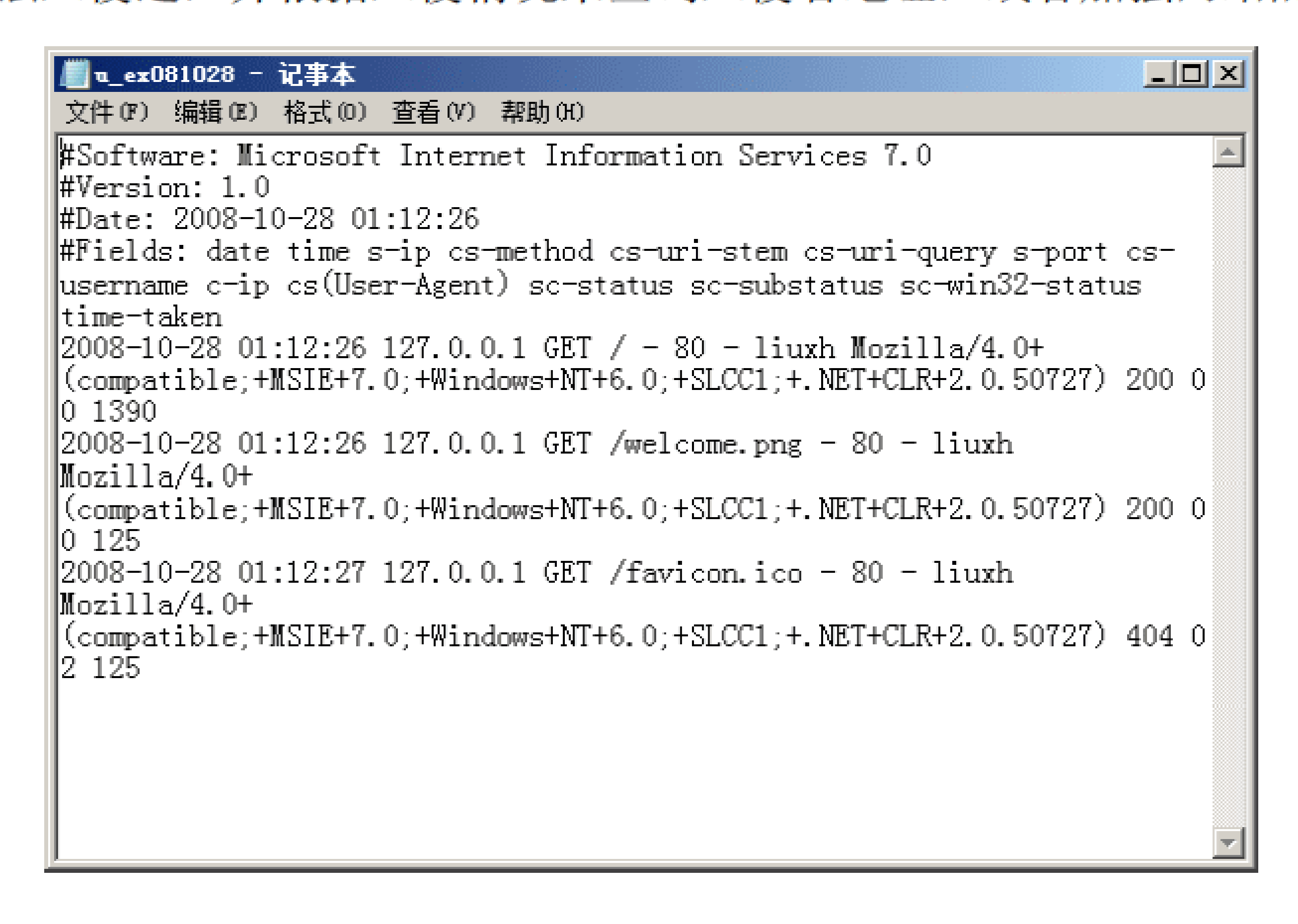


图 7-31 查看 Web 服务器事件日志

⑦ 设置完成后，在“操作”栏中单击“应用”链接，保存设置。

根据日志文件所在的目录，找到并打开日志文件，即可看到该日志文件记录的内容，如图 7-32 所示。根据日志文件中记录的内容，便可得知访问该站点的用户的详细情况，如 IP 地址、所访问过的文件等，还可以查出有哪些人非法入侵过，并根据入侵情况来查询入侵者地址，或者加强网站的安全措施。




```
#Software: Microsoft Internet Information Services 7.0
#Version: 1.0
#Date: 2008-10-28 01:12:26
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-
username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status
time-taken
2008-10-28 01:12:26 127.0.0.1 GET / - 80 - liuxh Mozilla/4.0+
(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+CLR+2.0.50727) 200 0
0 1390
2008-10-28 01:12:26 127.0.0.1 GET /welcome.png - 80 - liuxh
Mozilla/4.0+
(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+CLR+2.0.50727) 200 0
0 125
2008-10-28 01:12:27 127.0.0.1 GET /favicon.ico - 80 - liuxh
Mozilla/4.0+
(compatible;+MSIE+7.0;+Windows+NT+6.0;+SLCC1;+.NET+CLR+2.0.50727) 404 0
2 125
```

图 7-32　日志文件的内容

> **注意：**切勿混淆 IIS 站点活动日志与 Windows Server 2008 事件记录，IIS 中的日志记录功能用来记录用户与 Web 服务器间的活动，而 Windows 日志用来记录 Windows 系统中的活动情况，可以通过使用“事件查看器”来查看。

7.2.8　设置内容过期

“设置内容过期”是 Web 服务器重要的安全防护措施之一。对于时效性较强的数据信息(如会议通知、产品报价等)，可以通过设置内容过期来更新所发布的内容。浏览器会自动比较当前日期与截止日期，如果发现内容已过期则不再发布该数据，客户端也不会显示缓存页面而是从服务器更新。

① 在“Internet 信息服务(IIS)管理器”窗口的站点(以 Default Web Site 站点为例)主页中，双击“HTTP 响应标头”图标，显示如图 7-33 所示的“HTTP 响应标头”窗口。

② 在“操作”栏中，单击“设置常用标头”链接，显示如图 7-34 所示的“设置常用 HTTP 响应头”对话框。系统默认并未设置内容过期，选中“使 Web 内容过期”复选框，并设置相应过期方式即可。包括如下选项：

- 立即。使内容在传送后立即过期，该选项适用于包含不希望放入缓存或频繁更新的敏感信息的内容。
- 之后。设置内容在过期之前经过的时间，适用于定期更新的内容(如每日或每周更新的内容)。首先在对应的框中输入值，然后从列表中选择适当单位即可，如：“秒”、“分钟”、“小时”、“天”。
- 时间。设置内容过期时的准确日期和时间，适用于不希望频繁更改的内容。

③ 单击“确定”按钮，保存设置。

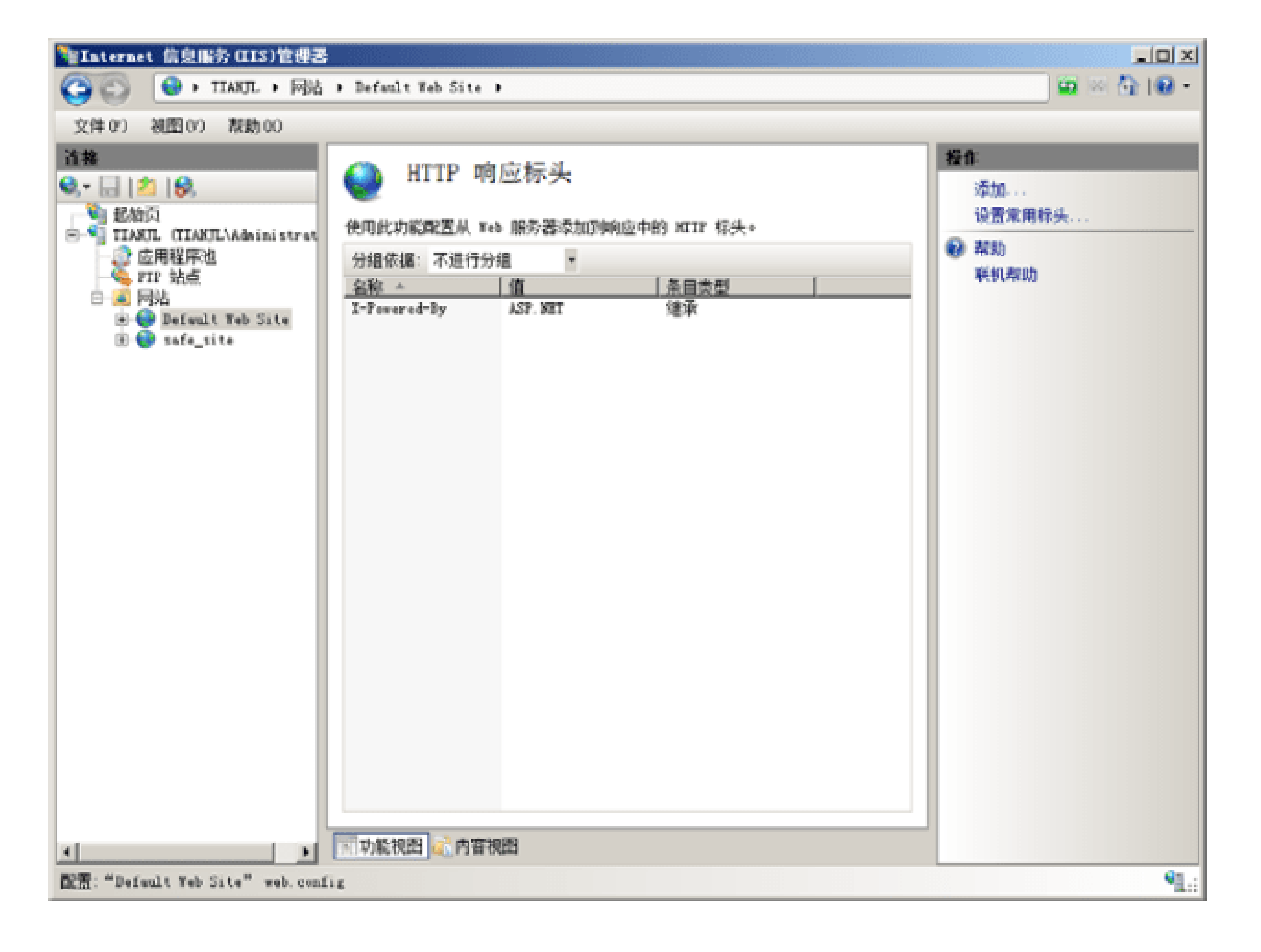


图 7-33 “HTTP 响应标头”窗口



图 7-34 “设置常用 HTTP 响应头”对话框

7.2.9 内容分级设置

IIS 7.0 中的托管模块设计给管理员的工作提供了极大的便利。.NET 信任级别功能可以托管模块、处理程序和应用程序指定信任的级别。通过用户组可以对一组用户进行分类，并对定义的用户组执行与安全相关的操作。需要注意的是，设置信任级别之前，必须先在“.NET 用户”窗口中，添加相关的用户角色，该功能需要 SQL Server 2005 数据库的支持。

① 在“Internet 信息服务(IIS)管理器”窗口的站点(以 Default Web Site 站点为例)主页中，双击“.NET 信任级别”图标，显示如图 7-35 所示的“.NET 信任级别”窗格。

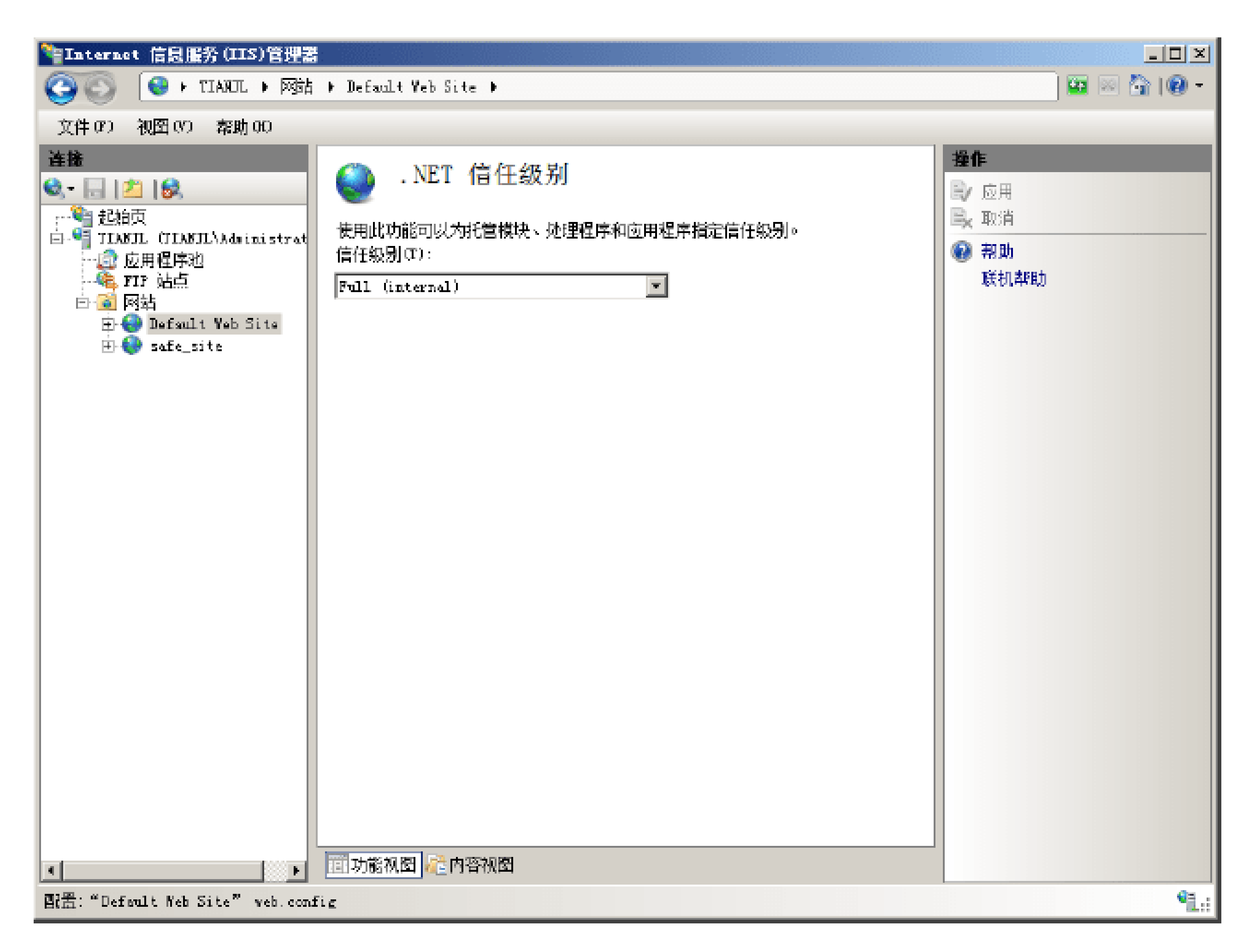


图 7-35 “.NET 信任级别”窗格

② 在“信任级别”下拉列表中，选择适当的信任级别即可，系统默认为“Full(internal)”级别。各个信任级别的具体含义如下。

- Full(internal)级别。指定不受限制的权限。授予 ASP.NET 应用程序权限，以便允许访问任何符合操作系统安全性的资源，支持所有特许操作。该信任级别是用于内部网络的 Web 站点，安全性最低。
- High(web_hightrust.config)。指定高级别的代码访问安全性，表示在默认情况下，应用程序无法执行下面任何一项操作：
  - 调用非托管代码。
  - 调用服务组件。
  - 向事件日志中写入内容。
  - 访问消息队列服务队列。
  - 访问 ODBC、OleDb 或 Oracle 数据源。
- Medium(web_mediumtrust.config)。指定中等级别的代码访问安全性，即默认情况下，除了高信任级别的限制以外，ASP.NET 应用程序还无法执行下面任何一项操作：
  - 访问应用程序目录范围之外的文件。
  - 访问注册表。
  - 进行网络或 Web 服务调用。
- Low(web_lowtrust.config)。指定低级别的代码访问安全性，表示在默认情况下，除了中等信任级别的限制以外，该应用程序还无法执行下面任何一项操作：
  - 向文件系统中写入内容。
  - 调用 Assert 方法。
- Minimal(web_minimaltrust.config)。指定最低级别的代码访问安全性，这表明该应用程序只具有执行权限，安全级别最高。

③ 在“操作”栏中，单击“应用”链接，保存设置即可。

7.2.10　注册 MIME 类型

MIME(Multipurpose Internet Mail Extensions)即多功能 Internet 邮件扩充服务，这是一种保证非 ASCII 码文件在 Internet 上传播的标准。如果 Web 服务器中没有添加相应的 MIME 类型，则用户无法访问该类型的文件。管理员可以对 IIS 全局定义 MIME 类型，也可以在网站、网站目录和网站虚拟目录级别上定义其他的 MIME 类型。

① 在“Internet 信息服务(IIS)管理器”窗口中，选择希望配置的站点或目录，双击“MIME 类型”图标，显示如图 7-36 所示的“MIME 类型”窗口，显示了系统已经集成的 MIME 类型。

② 在“操作”任务栏中单击“添加”按钮，显示如图 7-37 所示的“添加 MIME 类型”对话框。在“文件扩展名”文本框中输入欲添加的 MIME 类型，例如“.iso”，“MIME 类型”文本框中输入文件扩展名所属的类型。

③ 单击“确定”按钮，MIME 类型添加完成。如果还要添加其他 MIME 类型，可按如上步骤继续操作。



提示：如果希望处理所有文件而不考虑文件扩展名，则使用通配符“*”添加。

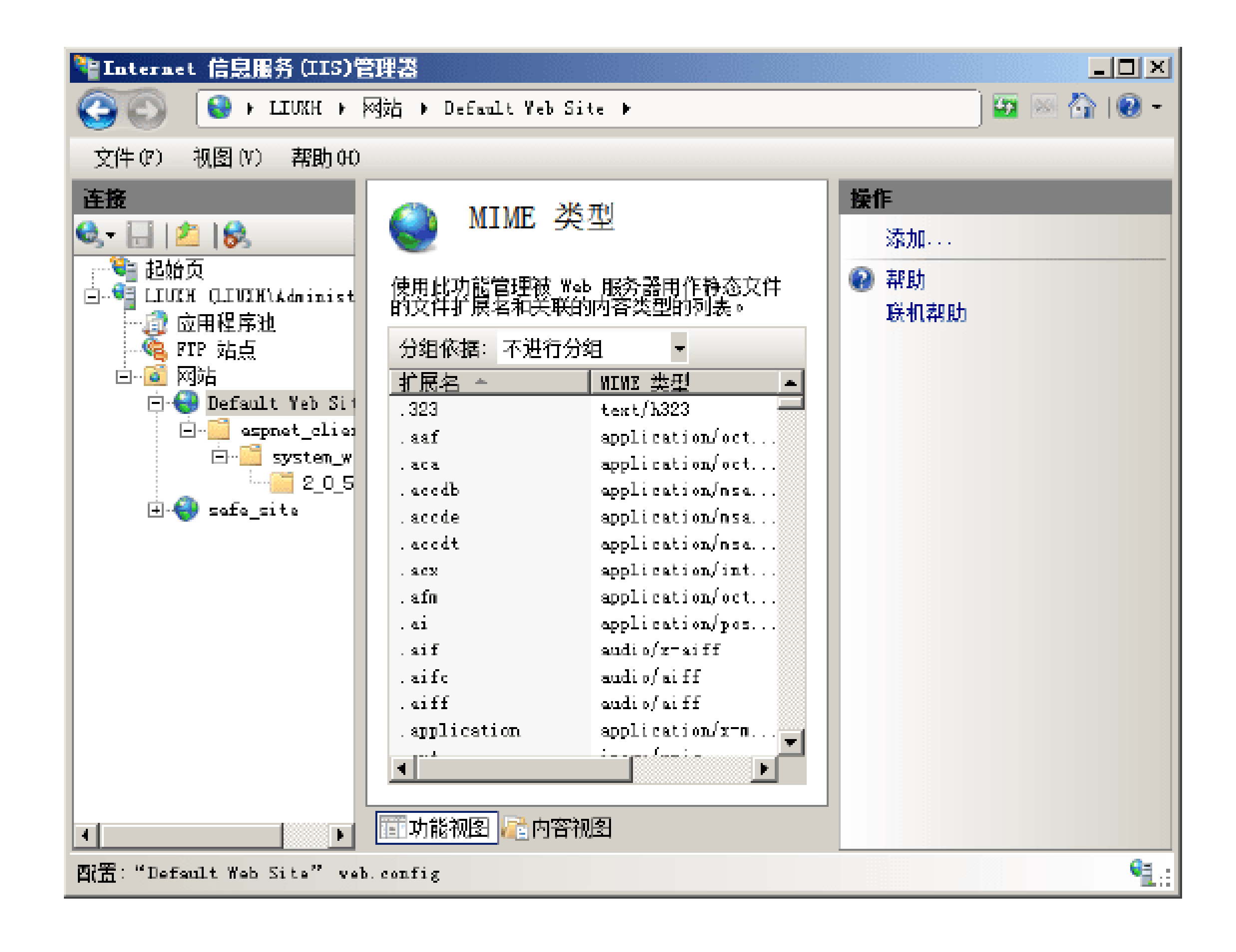


图 7-36　“MIME 类型”窗口

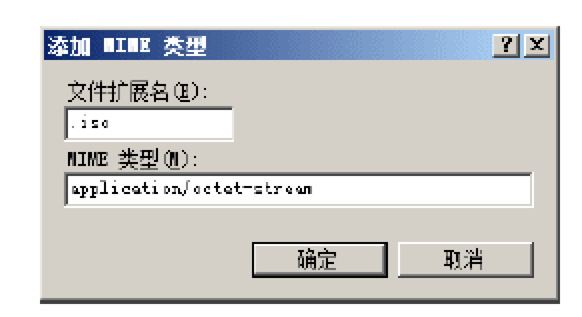


图 7-37　“添加 MIME 类型”对话框

7.3　FTP 服务安全

FTP 服务主要为用户提供上传和下载功能，客户端既可以从服务器下载文件到客户端，也可以从客户端将文件上传到服务器，利用 FTP 的这种功能，可以实现软件的下载、文件的交换与共享以及 Web 站点的维护等。基于 IIS 组件的 FTP 服务器，操作简便，运行稳定，是普通用户的首选方案。安装 IIS 7.0 过程中，默认没有安装 FTP 服务，用户需要手动添加。FTP 服务管理仍然采用 IIS 6.0 管理控制台，因此必须同时安装“IIS 6.0 管理兼容性”组件。

7.3.1　设置 TCP 端口

默认状态下，FTP 服务器使用 TCP 21 端口。通过修改服务端口也可以达到提高服务器安全的目的。此时，客户端若想连接到 FTP 服务器，不仅需要指定服务器的 IP 地址，还需要指定所使用的端口号，虽然访问过程有些繁琐，但可以从一定程度上拒绝客户端匿名链接。建议为安全需求较高的 FTP 服务器指定特殊 TCP 端口。

在“Internet 信息服务 (IIS)管理器”窗口中，展开“FTP 站点”项，右击“默认网站”项，在弹出的快捷菜单中选择“属性”命令，打开“默认 FTP 站点 属性”对话框，如图 7-38 所示。

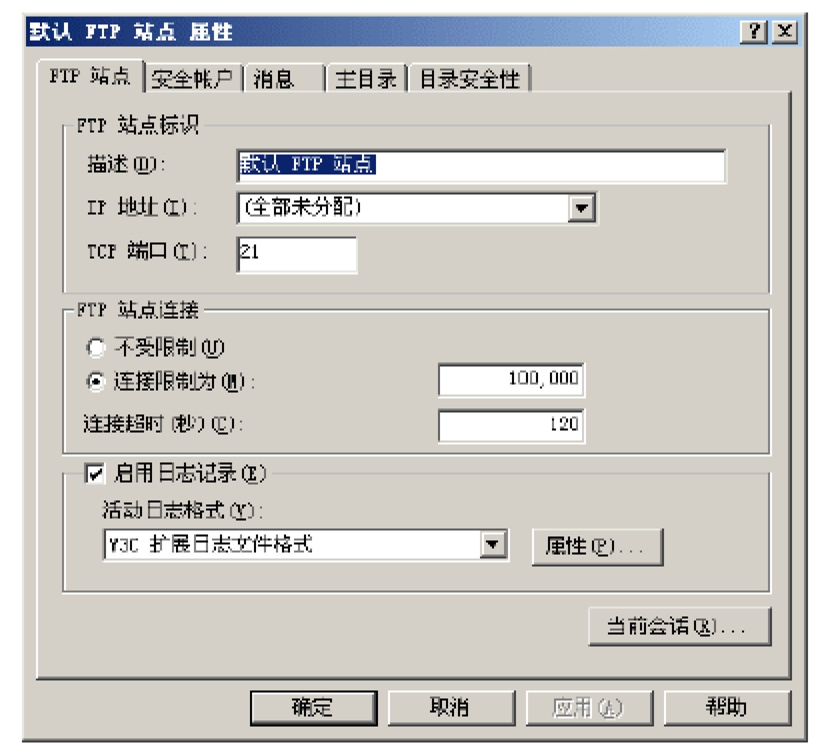


图 7-38　“默认 FTP 站点 属性”对话框

如果需要在拥有单个 IP 地址的服务器上发布多个 FTP 站点，则也可以通过修改 FTP 站点的 TCP 端口实现，只需为不同的站点指定相应的通信端口即可。

如果修改了默认的 FTP 端口，应当告知 FTP 客户，否则，访问请求将无法连接到该 FTP 服务器。例如，FTP 服务器的 IP 地址为 192.161.100.10，TCP 端口默认值为“21”，此时用户

只需通过客户端访问 ftp://192.161.100.10 即可访问该 FTP 网站，而如果指定了非“21”的端口号，如 1080，则只有访问 ftp://192.161.100.10:1080 时，才能实现对该网站的访问。

7.3.2　连接数量限制

当 FTP 服务器处于 Internet 环境中，或者提供大量的文件资源时，可能会产生大量的用户并发访问，如果服务器的配置比较低、性能比较差或 Internet 接入带宽比较小，则很容易导致系统响应迟缓或瘫痪，或者对企业的其他 Internet 服务(如 Web 服务、E-mail 服务等)造成严重影响，从而干扰其他网络服务的正常提供。尤其是对于一些小型企业而言，一般会在一台服务器上除了安装 FTP 服务外，同时还提供其他网络服务(如 Web、E-mail、Windows Media Services 等)，服务器无法同时处理过多的并发访问，从而导致所有服务的中断或超时。因此，这种情况下，就必须对 FTP 连接数量进行一定的限制。

在“FTP 站点”选项卡的“FTP 站点连接”选项区域中，可以设置连接是否受限制、限制的连接数量及连接超时，其中各选项的作用如下。

- 不受限制：不限制连接数量。适用于的服务器配置和网络带宽都较高，或者 FTP 服务仅为企业网络内部提供访问服务。
- 连接限制为：限制同时连接到该站点的连接数量，可指定该 FTP 站点所允许连接的最大数值。
- 连接超时：设置服务器断开未活动用户的时间(以秒为单位)，从而确保及时关闭失败的连接，或者长时间没有活动的连接，及时释放系统性能和网络带宽，减少无谓的系统资源和网络资源浪费。默认连接超时为 120 s。

7.3.3　用户访问安全

由于 FTP 站点中往往存储着非常重要的文件或应用程序，甚至是 Web 网站的全部内容，所以，FTP 站点的访问安全显得尤其重要。因此，对于一些比较特殊的 FTP 站点，必须进行用户身份验证，并限制允许访问该 FTP 服务的 IP 地址，从而确保 FTP 站点的安全。

1.　禁止匿名访问

默认状态下，FTP 站点是允许用户进行匿名连接的，即所有用户都无需经过身份认证，就可以查看、读取并下载 FTP 站点上的所有内容。如果 FTP 站点中存储有重要的或比较敏感的信息，只允许授权用户访问，那么就应当禁用匿名访问。

① 打开 FTP 站点属性对话框，切换至“安全账户”选项卡，取消选中“允许匿名连接”复选框，显示如图 7-39 所示的“IIS6 管理器”对话框。

② 单击“是”按钮，关闭“IIS6 管理器”对话框。在“安全账户”选项卡中，单击“确定”按钮，即可禁止用户匿名访问该 FTP 站点，如图 7-40 所示。

当禁止用户匿名连接后，只有服务器或活动目录中有效的账户，才能通过身份认证，并实现对该 FTP 站点的访问。

除禁止匿名连接外，还可以在本地计算机或域控制器上，创建专用于 FTP 连接的匿名用户账户(区别于系统默认的 IUSR_服务器名账户)，对其在 FTP 主目录或单个文件夹的权限进行限制，实现 FTP 服务器的安全。选中“允许匿名连接”复选框，单击“浏览”按钮，选择指定用户账户即可。单击“应用”按钮，系统将自动添加对应账户的密码，如图 7-41 所示。如果选择“只允许匿名连接”复选框，则用户将无法使用

用户名和密码登录 FTP 服务器。此选项拒绝访问使用具有管理凭据账户的那些用户，而只为使用匿名访问账户的用户指派访问权限。



图 7-39　“IIS6 管理器”对话框

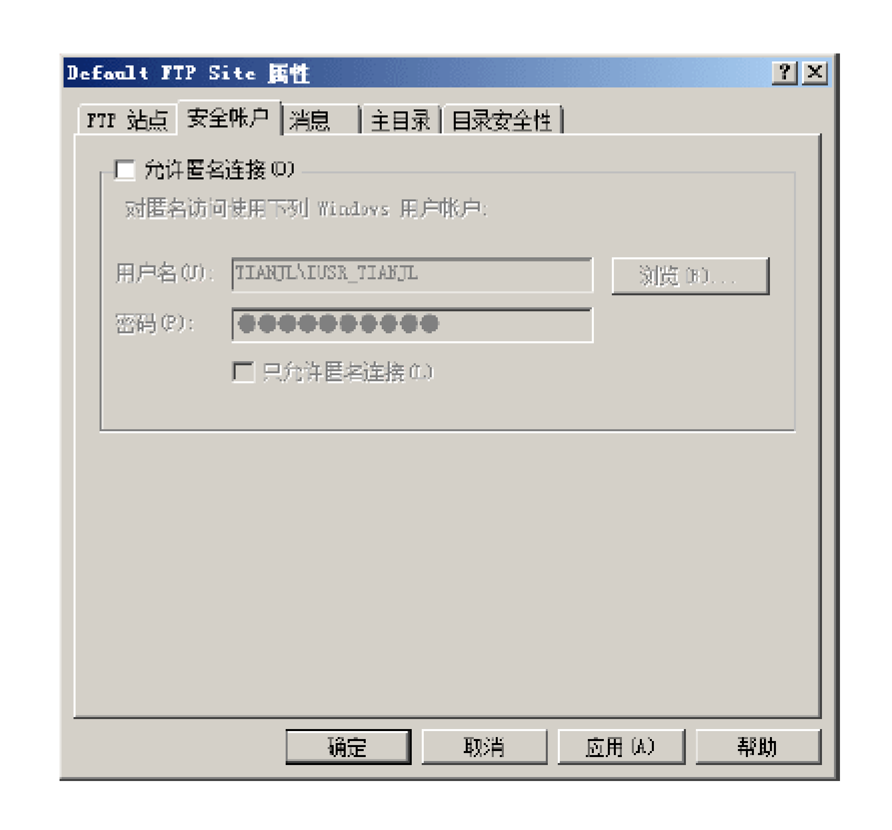


图 7-40　“安全账户”选项卡

2.　限制 IP 地址

通过对 IP 地址的限制，可以只允许或拒绝某些特定范围内的计算机访问该 FTP 站点，从而可以在很大程度上避免来自外界的恶意攻击，并且将授权用户限制在某一个范围。将 IP 地址限制与用户认证访问结合在一起，将进一步提高 FTP 站点访问的安全性。特别是对于企业内部的 FTP 站点而言，采用 IP 地址限制的方式，是非常简单而有效的。

① 打开 FTP 站点属性对话框，切换到“目录安全性”选项卡，如图 7-42 所示，选择“拒绝访问”单选按钮，表示默认情况下所有计算机均被拒绝访问，只有将要添加的 IP 地址用户可以访问。相反，也可以设置为默认情况下所有计算机都将被“允许访问”，然后创建需要拒绝访问的 IP 地址列表。

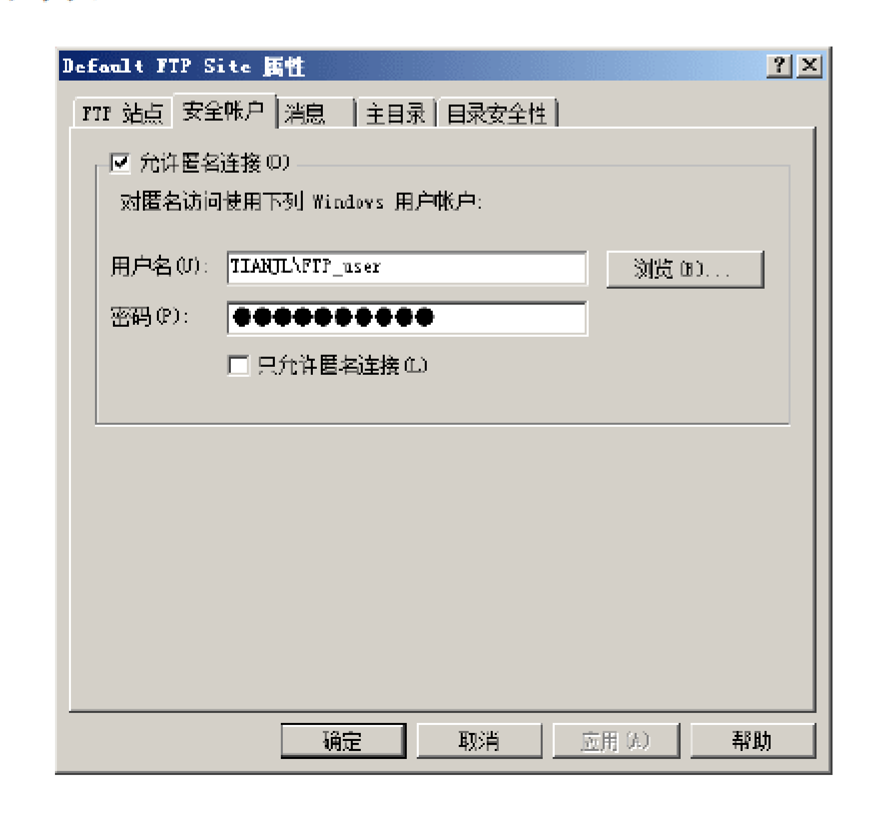


图 7-41　更改匿名连接账户

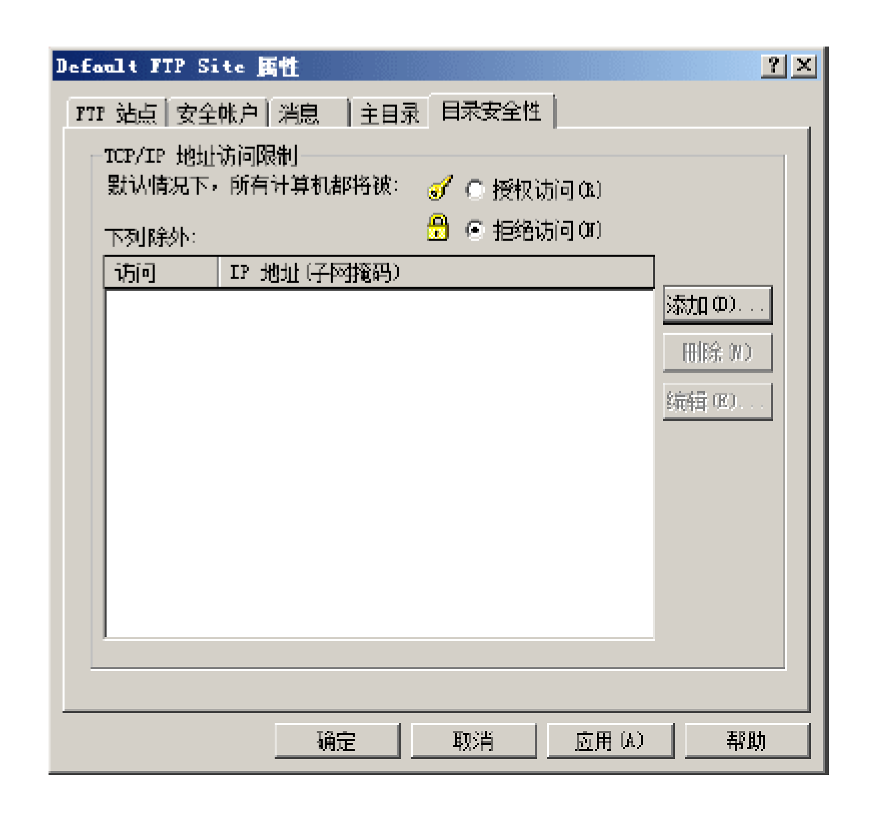


图 7-42　“目录安全性”选项卡

② 单击“添加”按钮，显示如图 7-43 所示的“授权访问”对话框，默认选择“一台计算机”单选按钮，每次只能添加一个 IP 地址。建议选择“一组计算机”单选按钮，在“网络标识”和“子网掩码”文本框中，输入相应的网络标识信息，添加一个网段内的所有 IP 地址。

③ 单击“确定”按钮，将该所选 IP 地址或 IP 地址段添加至“下列除外”列表中，如图 7-44 所示。

创建“拒绝访问”IP 地址列表的方法与之相同，此处不再赘述。

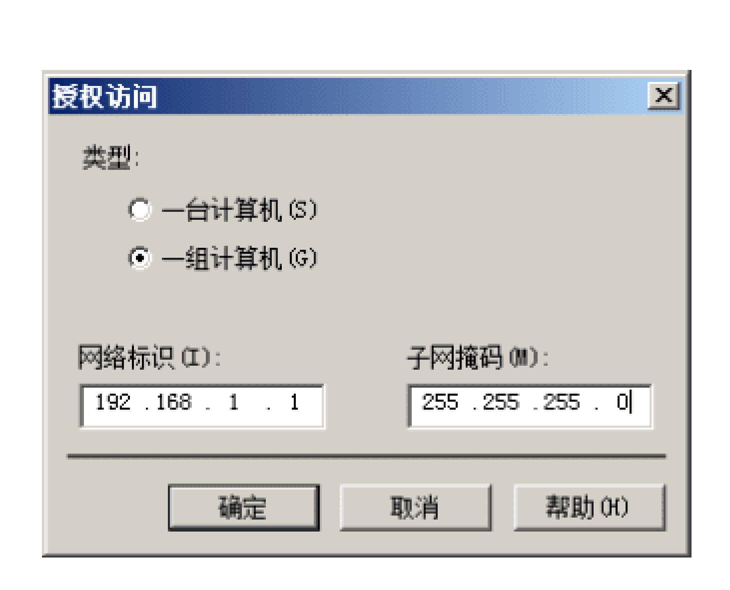


图 7-43　“授权访问”对话框

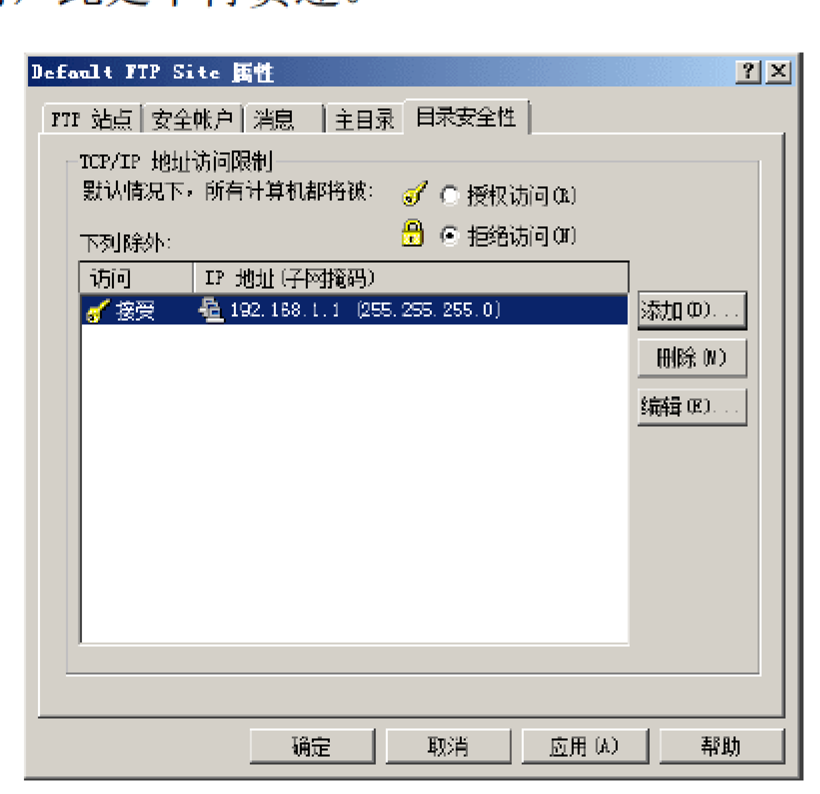


图 7-44　创建成功的授权访问 IP 地址

④　单击“确定”按钮，保存设置即可。

7.3.4　文件访问安全

在 FTP 站点属性的“主目录”对话框中，可以修改文件的访问权限。默认情况下，匿名用户均拥有“读取”权限，如图 7-45 所示。

若欲将该 FTP 站点作为为匿名用户提供的文件下载服务器，可以保持系统默认设置，即允许任何用户匿名访问该 FTP 站点，并且拥有读取该 FTP 站点的权限。

若欲将该 FTP 站点作为为授权用户提供的文件下载服务器，可以赋予该站点主目录以“读取”权限，禁止匿名访问，并设置采用何种方式实施身份认证。

若欲将该 FTP 站点作为上传文件服务器，则应当赋予该站点“读取”和“写入”权限，禁止匿名访问，并设置采用何种方式实施身份认证。否则，所有匿名用户都将拥有“写入”权限，从而造成 FTP 系统安全危机。

图 7-45　“主目录”选项卡

需要注意的是，在设置 FTP 访问权限后，还必须为该主目录设置 NTFS 访问权限，以确保用户拥有相应的访问权限。同时，还应当设置磁盘配额，以防止被授予写权限的用户滥用磁盘空间。

7.4　终端服务安全

终端服务网关(TS 网关)可以使授权用户从远程任何位置连接到 Internet，并且可以运行远程桌面连接(RDC)客户端的设备，连接到内部企业网络或专用网络上的资源。网络资源可以是终端服务器、运行 RemoteApp 程序的终端服务器或启用了远程桌面的计算机。

7.4.1 TS 网关概述

TS 网关使用 HTTPS 上的远程桌面协议(RDP)在 Internet 上的远程用户与运行其生产力应用程序的内部网络资源之间建立安全的加密连接。

TS 网关有许多优点，具体包括如下内容：

- 通过 TS 网关，远程用户可以使用加密连接，通过 Internet 连接到内部网络资源，而不必配置虚拟专用网络(VPN)连接。
- TS 网关提供全面的安全配置模型，可以控制对特定内部网络资源的访问。TS 网关提供点对点的 RDP 连接，而不是允许远程用户访问所有内部网络资源。
- 通过 TS 网关，大多数远程用户可以连接到在专用网络中的防火墙后面或跨网络地址转换程序(NAT)托管的内部网络资源。此时，通过 TS 网关，不必对 TS 网关服务器或客户端执行其他配置。通常情况下，Windows 系统会采用安全措施来阻止远程用户跨防火墙和 NAT 连接到内部网络资源。这主要是出于网络安全考虑，通常会阻止端口 3389(用于 RDP 连接的端口)。TS 网关使用 HTTP 安全套接字层/传输层安全(SSL/TLS)隧道将 RDP 通信传输到端口 443。这主要是因为，443 端口默认是开启状态的，所以 TS 网关利用此网络设计提供跨多个防火墙的远程访问连接。
- 通过 TS 网关管理器管理单元控制台可以配置授权策略，以定义远程用户要连接到内部网络资源必须满足的条件。例如，可以指定可以连接到内部网络资源的用户和可以连接到的网络资源等。

若要正常使用 TS 网关，必须满足下列先决条件：

- 在服务器上安装 Windows Server 2008 操作系统。
- 配置为 TS 网关的用户，必须是服务器计算机上 Administrators 组的成员。
- 必须为 TS 网关服务器获取安全套接字层(SSL)证书(如果还没有该证书)。默认情况下，在 TS 网关服务器上，RPC/HTTP 负载平衡服务和 Internet 信息服务(IIS)使用传输层安全(TLS)1.0 对通过 Internet 在客户端与 TS 网关服务器之间进行的通信加密。若要正常使用 TLS，必须在 TS 网关服务器上安装 SSL 证书。
- 如果配置的 TS 网关授权策略要求客户端计算机上的用户是 Active Directory 安全组的成员，才能连接到 TS 网关服务器，或如果要部署负载平衡的 TS 网关服务器群集，则 TS 网关服务器必须也是 Active Directory 域的成员。



注意：为了进一步保证服务器的安全，建议为终端服务创建一个专用的安全组，并将具有访问权限的用户添加到该安全组中，这里添加名为“TSGW”的安全组。

7.4.2 安装 TS 网关

终端服务网关组件，可以与终端服务共同安装在同一台服务器上，也可以安装在不同的服务器上，这里在一台服务器上同时安装终端服务和终端服务网关组件。建议不要将终端服务网关与域控制器安装在同一台服务器上。具体操作步骤如下：

① 打开“服务器管理器”窗口，在左侧栏中依次展开“服务器管理器”→“角色”→“终端服务”，如图 7-46 所示。

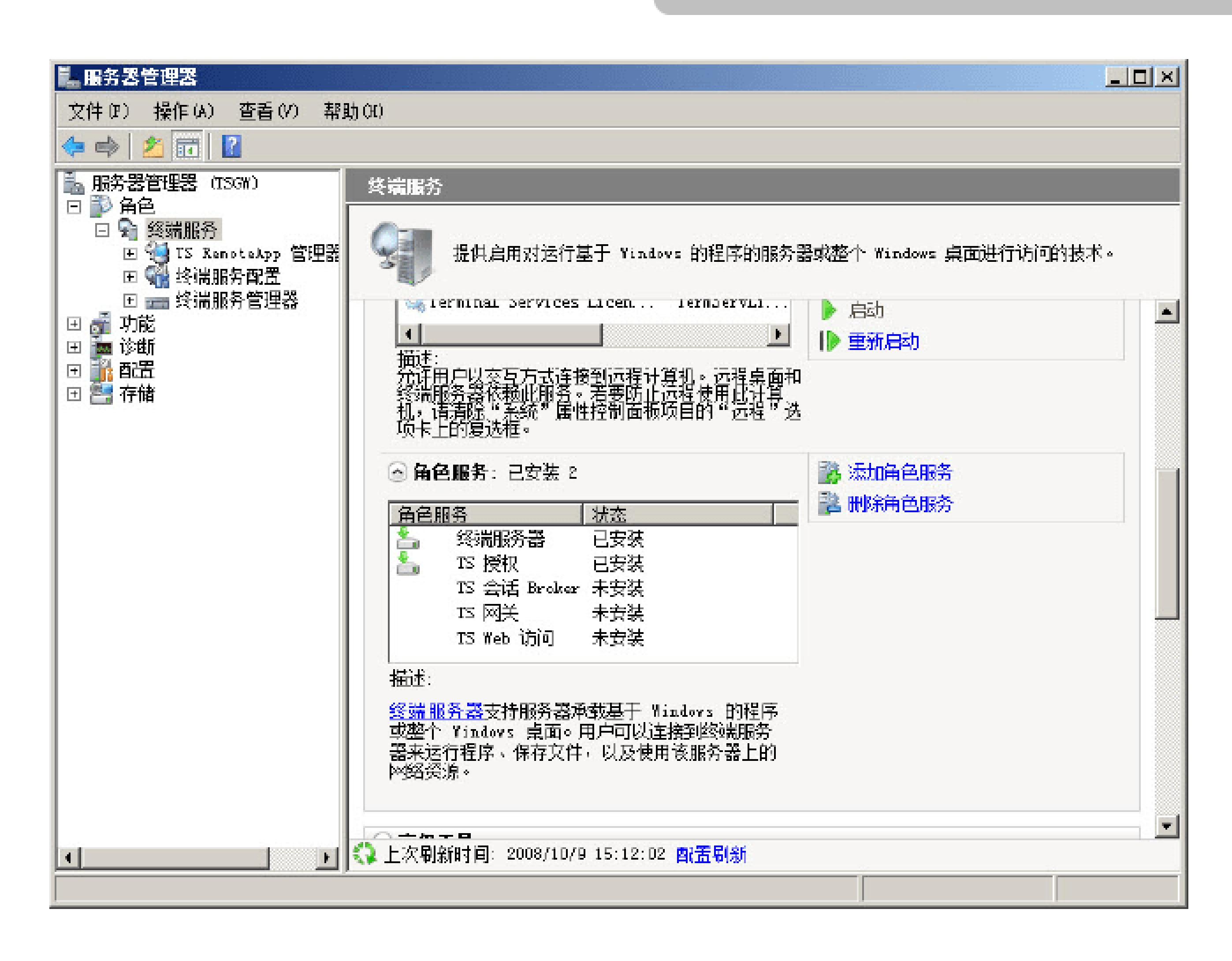


图 7-46　“服务器管理器”窗口

② 在右侧窗口中，单击“添加角色服务”按钮，显示如图 7-47 所示的“选择角色服务”界面。

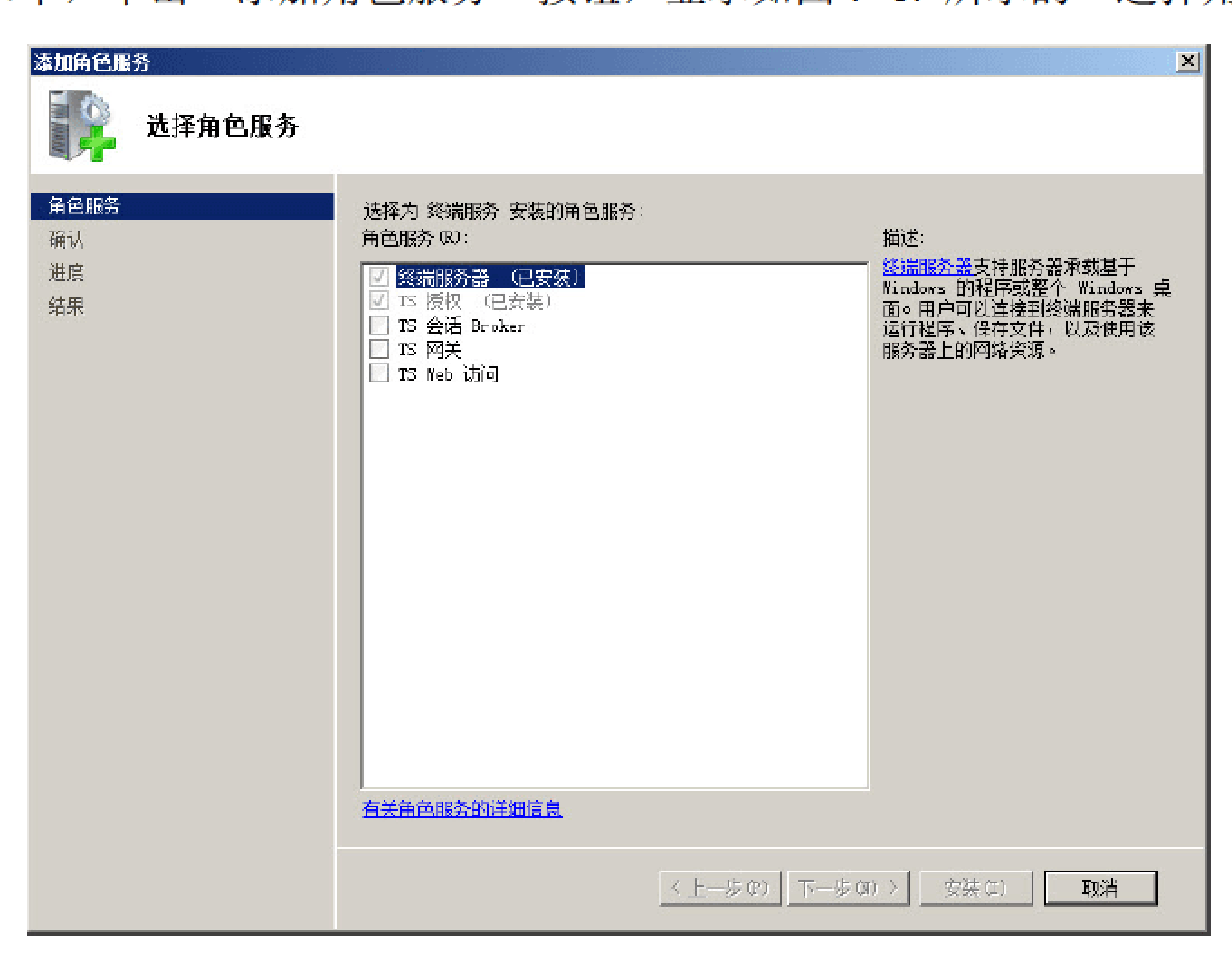


图 7-47　“选择角色服务”界面

③ 选中“TS 网关”复选框，显示如图 7-48 所示的“是否添加 TS 网关所需的角色服务和功能？”界面，提示安装所必需的 IIS 组件。

④ 单击“添加必需的角色服务”按钮，返回“选择角色服务”对话框，单击“下一步”按钮，显示如图 7-49 所示的“选择 SSL 加密的服务器身份验证证书”界面。与客户端进行通信时，TS 网关需要使用安全套接字层协议来加密网络通信，在这里可以根据需要设置所使用的证书，这里选择“稍后为 SSL 加密选择证书”单选按钮，稍后再设置所使用的证书。

⑤ 单击“下一步”按钮，显示如图 7-50 所示的“为 TS 网关创建授权策略”界面。终端服务的连接授权策略(TS CAP)允许指定可连接到该 TS 网关服务器的用户，这里选择“以后”单选按钮，在稍后的操作中再进行设置。

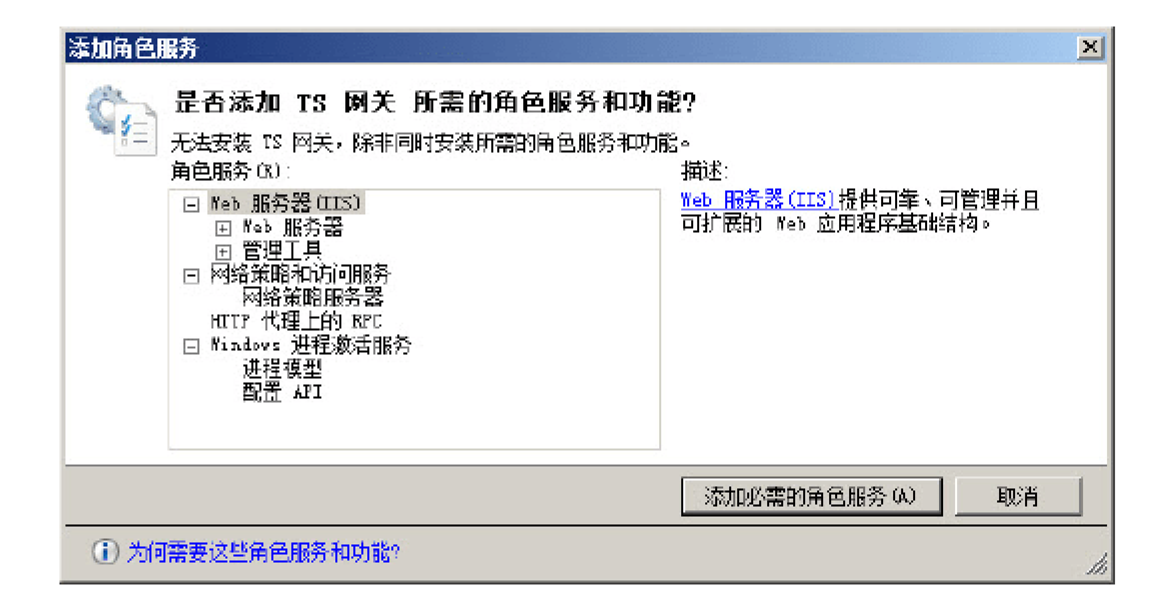


图 7-48 “是否添加 TS 网关所需的角色服务和功能？”界面



图 7-49 “选择 SSL 加密的服务器身份验证证书”界面



图 7-50 “为 TS 网关创建授权策略”界面

⑥ 单击“下一步”按钮，显示如图 7-51 所示的“网络策略和访问服务”界面，显示网络策略和访问服务的简介内容。

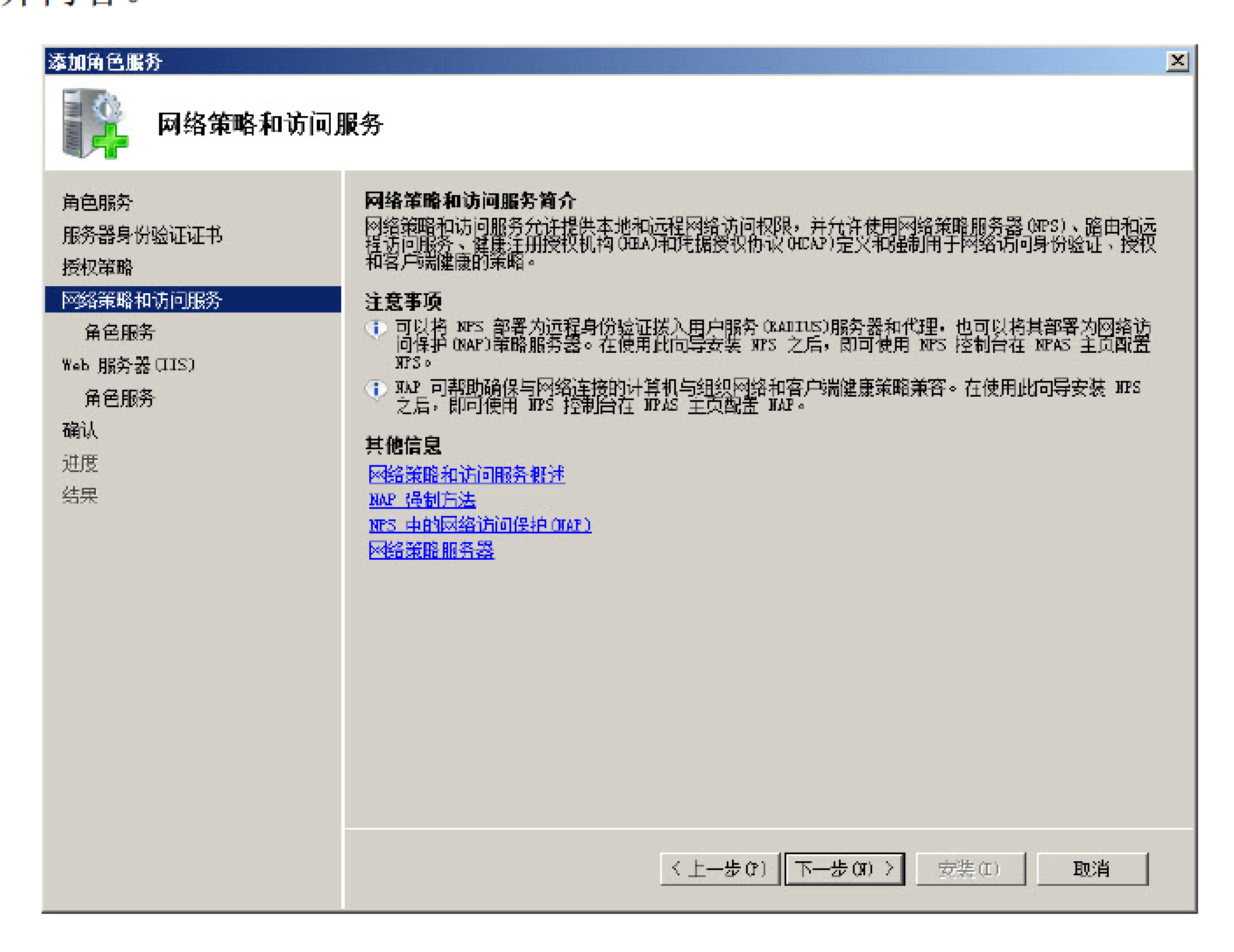


图 7-51 “网络策略和访问服务”界面

⑦ 单击“下一步”按钮，显示如图 7-52 所示的“选择角色服务”界面。因为 TS 网关需要使用网络策略服务，因此必须安装“网络策略服务器”角色服务。如果服务器中已经安装了该角色服务，则不会显示该对话框。

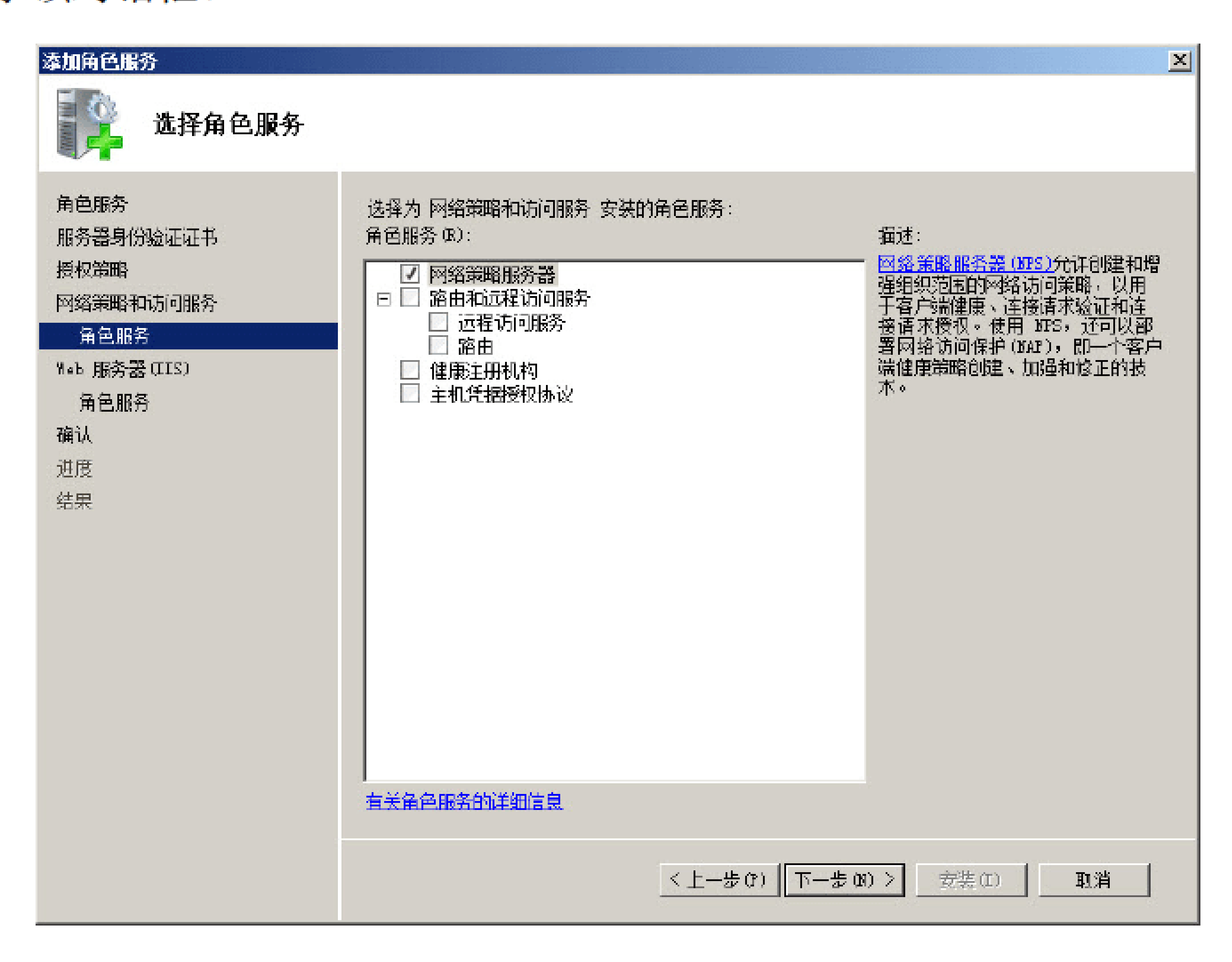


图 7-52 “选择角色服务”界面

⑧ 单击“下一步”按钮，显示如图 7-53 所示的“Web 服务器(IIS)”界面，显示 Web 服务器的简介内容。

⑨ 单击“下一步”按钮，显示如图 7-54 所示的“选择角色服务”界面。显示了所要安装的 Web 服务器的角色服务，保持默认设置即可。



图 7-53 “Web 服务器(IIS)”界面

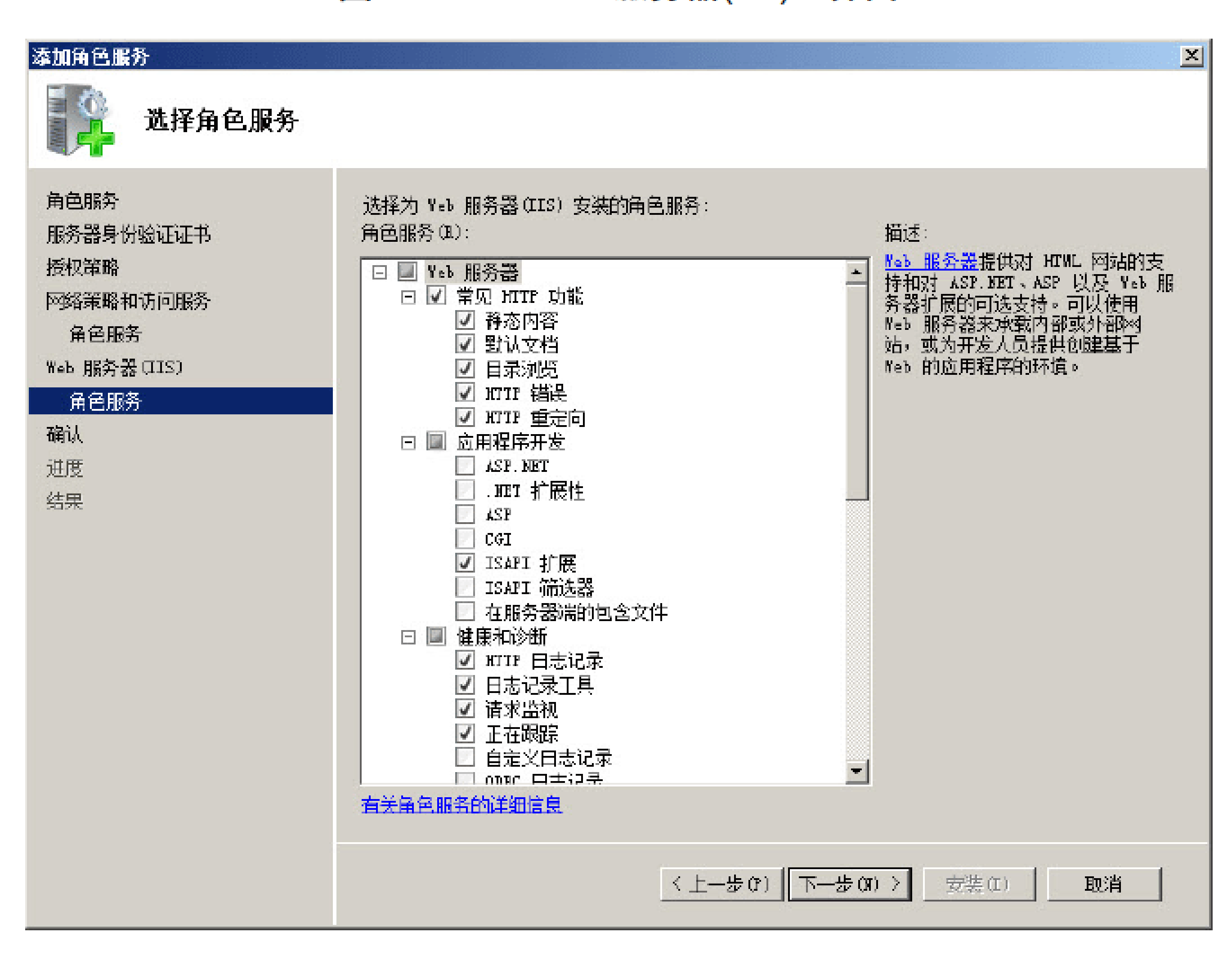


图 7-54 “选择角色服务”界面

⑩ 单击“下一步”按钮，显示如图 7-55 所示的“确认安装选择”界面。检查设置是否正确，单击“上一步”按钮，可以返回重新设置。

⑪ 单击“安装”按钮，开始安装 TS 网关。安装完成后，显示如图 7-56 所示的“安装结果”界面，提示所需的角色服务已经安装成功。

⑫ 单击“关闭”按钮，完成并退出安装向导。

依次选择“开始”→“管理工具”→“终端服务”→“TS 网关管理器”，显示如图 7-57 所示的“TS 网关管理器”窗口。



图 7-55　“确认安装选择”界面



图 7-56　“安装结果”界面

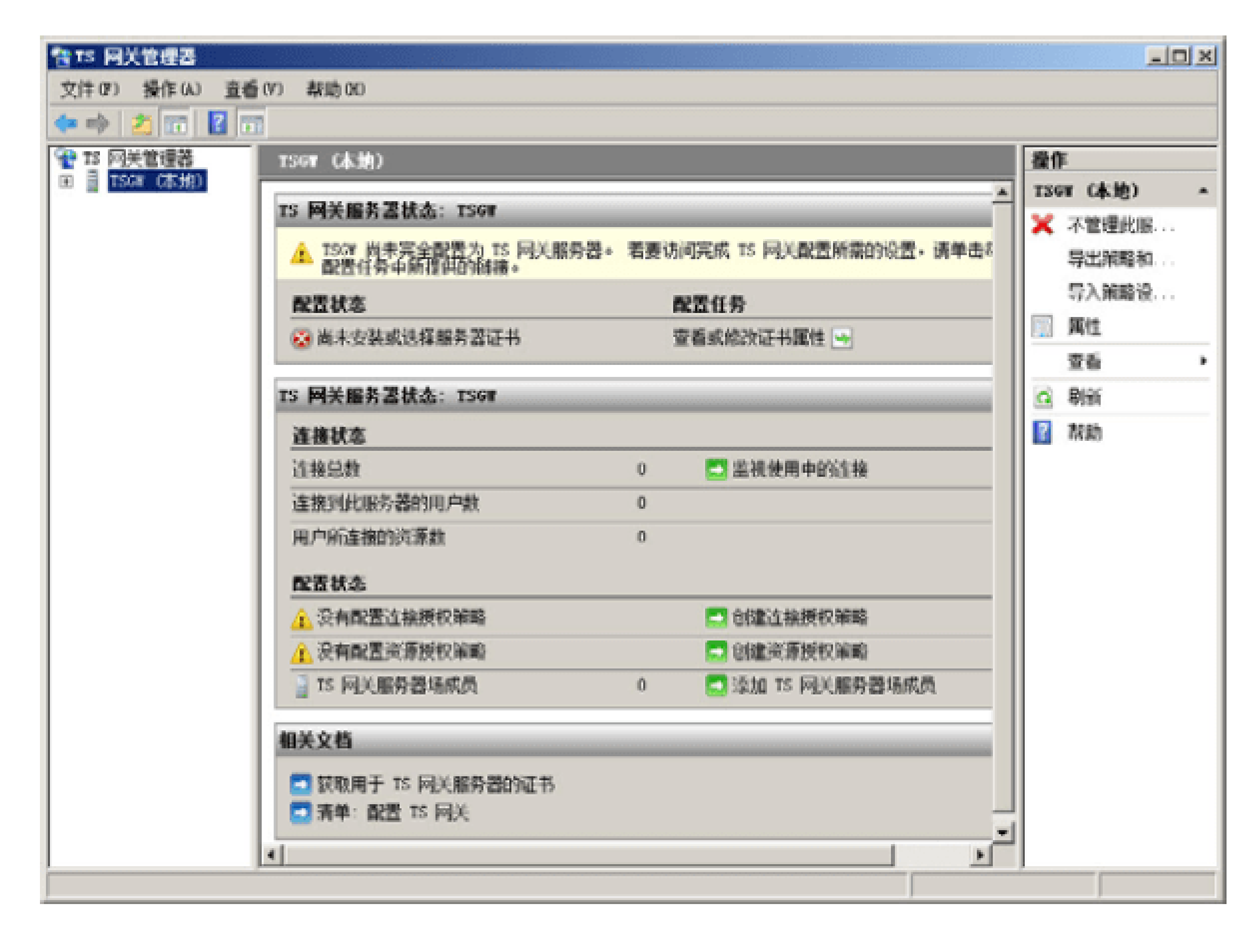


图 7-57　“TS 网关管理器”窗口

7.4.3 为 TS 网关服务器获取证书

默认情况下，使用传输层安全(TLS)1.0 加密，通过 Internet 在终端服务客户端与 TS 网关服务器之间进行的通信。若要正常使用 TLS，必须在 TS 网关服务器上安装与安全套接字层兼容的 X.509 证书。

通常情况下，服务器可以通过以下几种方法获取证书：

- 从独立证书颁发机构(CA)或企业证书颁发机构获取证书。
- 向参与 Microsoft 根证书程序成员计划的任一受信任公用 CA 购买证书(或免费获取一个试用版)。
- 在安装 TS 网关角色服务时，使用添加角色向导创建自签名证书，或在安装 TS 网关后，使用 TS 网关管理器创建自签名证书。

这里使用第三种方法，使用 TS 网关管理器创建自签名证书。

① 这里并没有创建任何证书，因此会在 TS 网关管理器窗口中，提示尚未安装或选择服务器证书。在“TS 网关管理器”窗口中，单击“查看或修改证书属性”显示如图 7-58 所示的“TSGW 属性”对话框。

② 单击“创建证书”按钮，显示如图 7-59 所示的“创建自签名证书”对话框。在“证书名称”下，输入自签名证书名称。需要注意的是，该名称必须与客户端连接到 TS 网关服务器时使用的 DNS 名称相同，这里保持默认设置。在“文件名”文本框中，可以根据需要设置该证书的保存目录。如果选中“存储根证书”复选框，则会在创建完成后，提示 TS 网关已成功地创建自签名证书，并确认已存储的证书的位置。

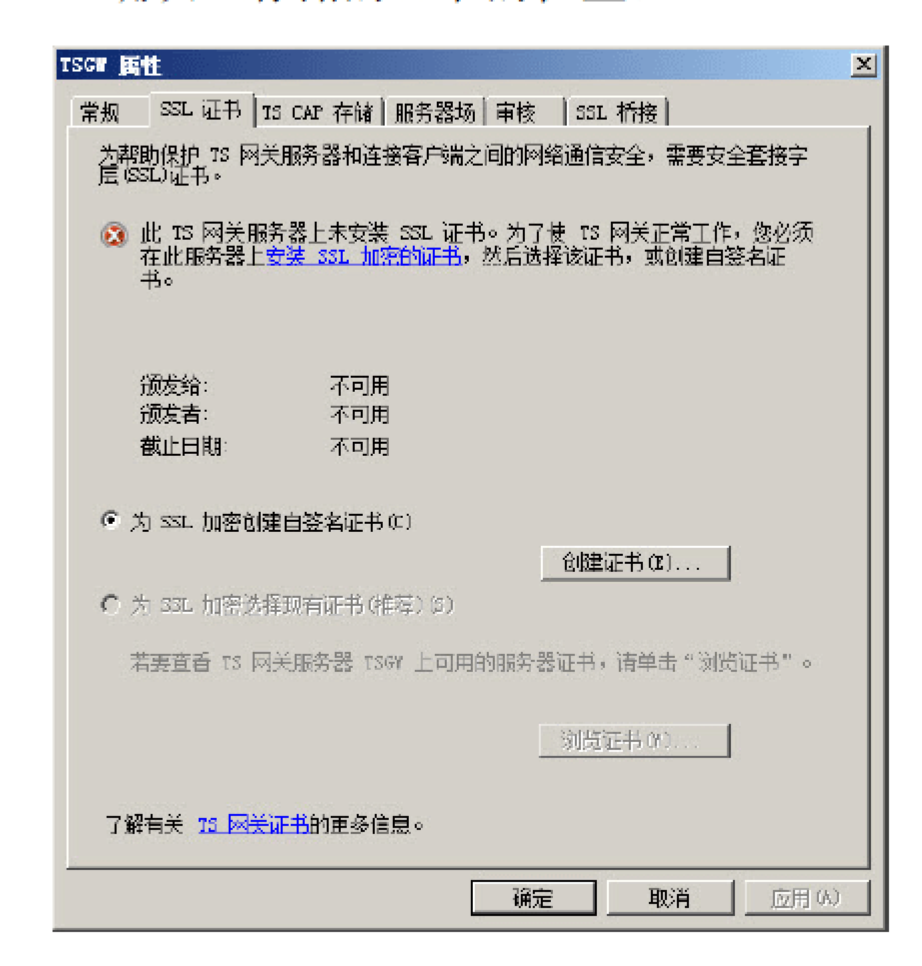


图 7-58 “TSGW 属性”对话框

图 7-59 “创建自签名证书”对话框

③ 单击“确定”按钮，显示如图 7-60 所示的“TS 网关”对话框。提示已成功创建自签名证书，以及该证书的保存位置。

④ 单击“确定”按钮，返回“TSGW 属性”对话框，再次单击“确定”按钮，保存设置即可。



图 7-60 “TS 网关”对话框



提示：对于该证书，在域环境中，管理员可以使用组策略将该证书发布在网络中的计算机上。

7.4.4　创建终端服务策略

创建终端服务策略包括管理终端服务连接授权策略(TS CAP)和管理终端服务资源授权策略(TS RAP)两部分。终端服务连接授权策略的作用是检查连接的用户是否必须符合特定的要求，只有符合连接授权策略的用户，才能连接到 TS 网关。管理终端服务资源授权策略的作用是指定远程用户可通过 TS 网关服务器连接到的内部网络资源(计算机)。

创建终端服务策略的具体操作步骤如下：

① 在“TS 网关管理器”窗口中，右击“策略”并在快捷菜单中选择“新建授权策略”选项，显示如图 7-61 所示的“为 TS 网关创建授权策略”界面。为了操作简单，建议选择“创建 TS CAP 和 TS RAP(推荐)”单选按钮，同时创建终端服务连接授权策略和管理终端服务资源授权策略。

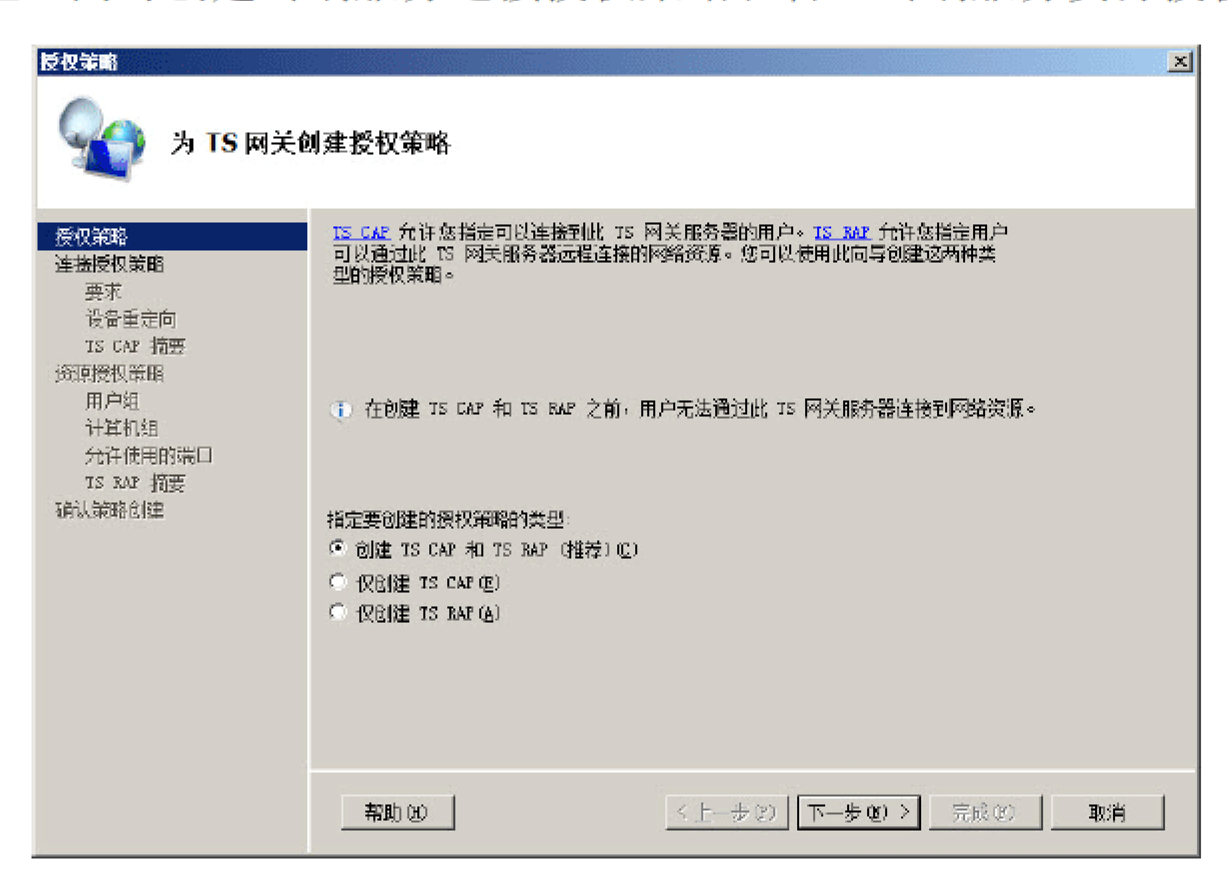


图 7-61　“为 TS 网关创建授权策略”界面

② 单击“下一步”按钮，显示如图 7-62 所示的设置 TS CAP 界面。在“输入 TS CAP 的名称”文本框中，输入授权策略的名称。

③ 单击“下一步”按钮，显示如图 7-63 所示的设置身份验证方法对话框。根据需要设置 Windows 身份验证方法，包括“密码”和“智能卡”两种方法。可以只使用一种方法，也可以同时使用两种方法，此时可以使用任意一种方法进行身份验证。

④ 在“用户组成员身份(必需)”文本框右侧单击“添加组”按钮，显示如图 7-64 所示的“选择组”对话框。在“输入对象名称来选择”文本框中，输入想要设置的用户组，单击“检查名称”按钮，检查组名是否正确。

⑤ 单击“确定”按钮，返回设置身份验证方法对话框，单击“下一步”按钮，显示如图 7-65 所示的“为 TS 网关创建 TS CAP”界面。根据需要设置客户端设备的设备重定向，这里选择“启用所有客户端设备的设备重定向”单选按钮。

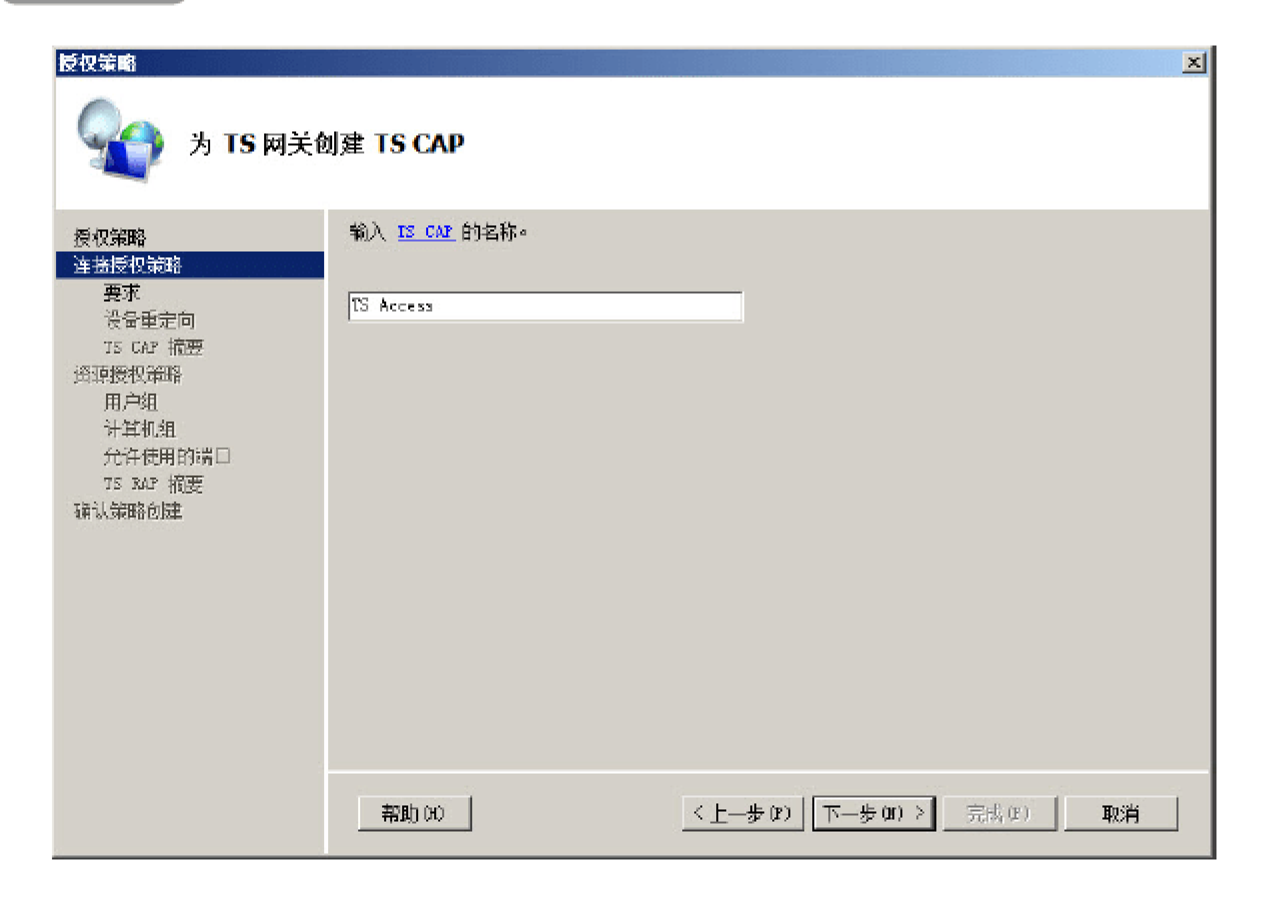


图 7-62　设置 TS CAP



图 7-63　设置身份验证方法

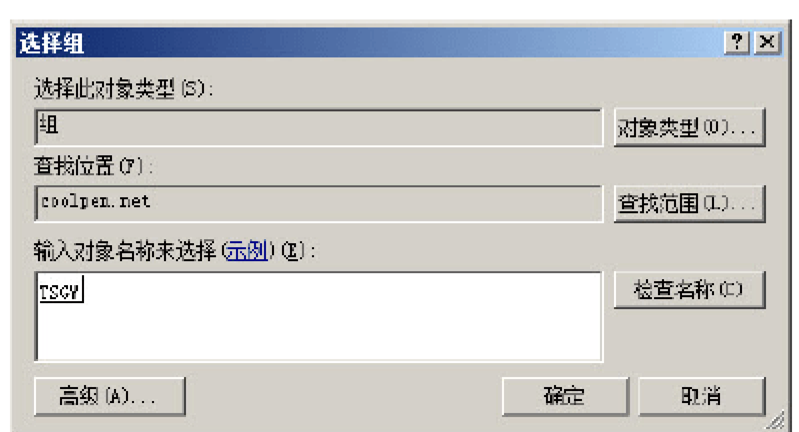


图 7-64　“选择组”对话框

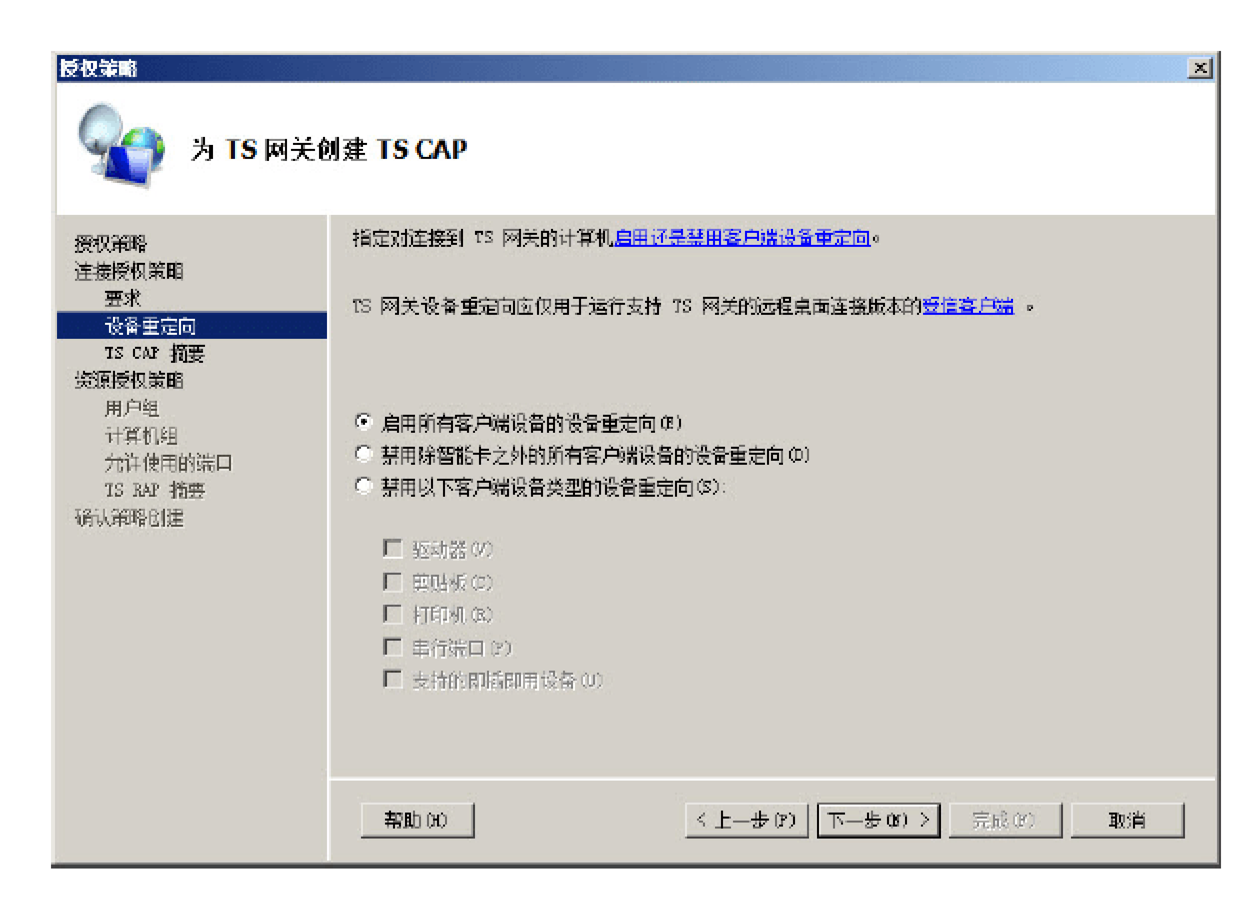


图 7-65　设置客户端设备重定向

⑥ 单击“下一步”按钮，显示如图 7-66 所示的“TS CAP 设置摘要”界面。检查前面的设置是否正确，单击“上一步”按钮，可以返回重新设置。

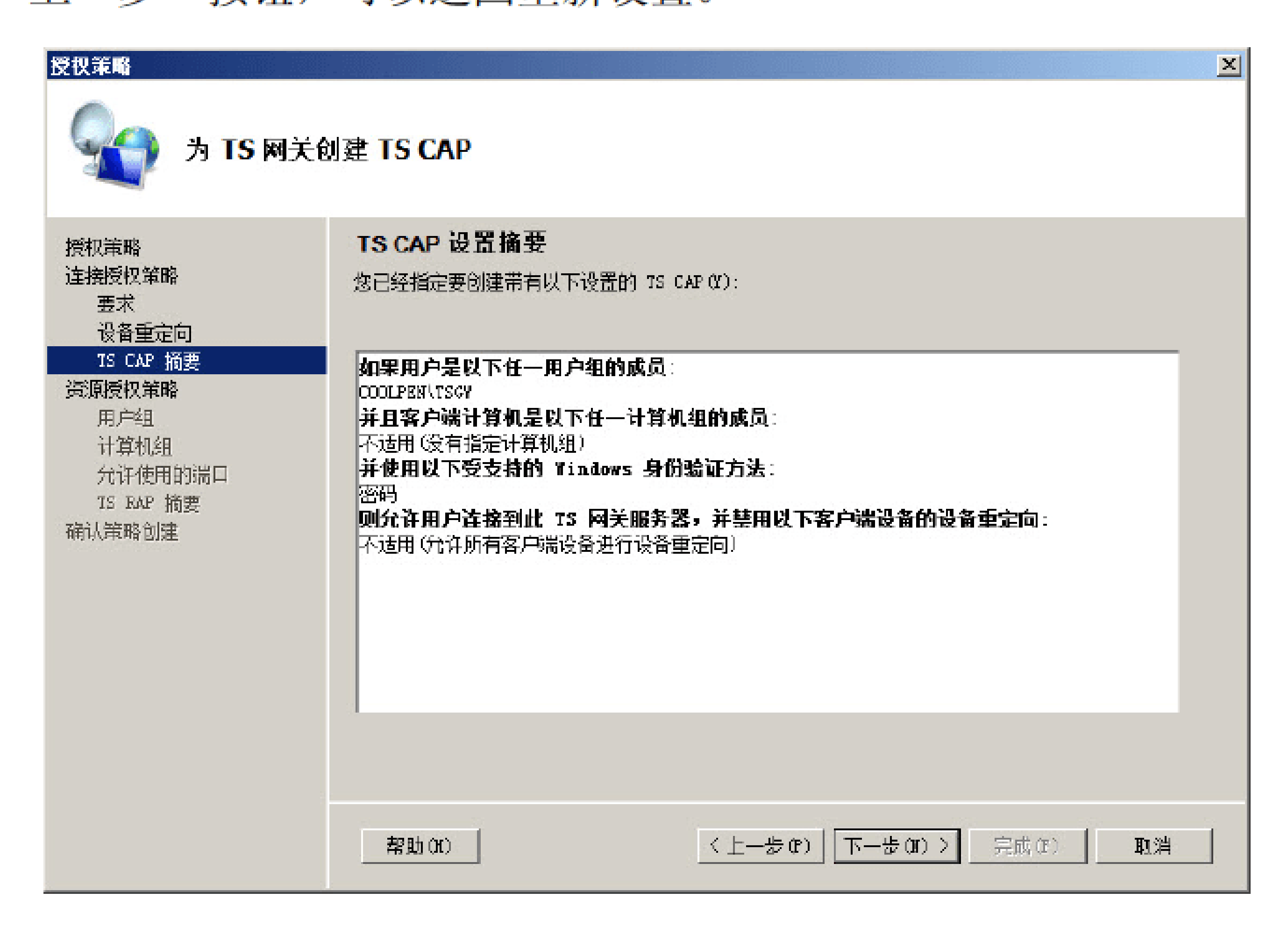


图 7-66　“TS CAP 设置摘要”界面

⑦ 单击“下一步”按钮，显示如图 7-67 所示的设置 TS RAP 名称对话框。在“输入 TS RAP 的名称”文本框中，输入所创建的 TS TAP 的名称。

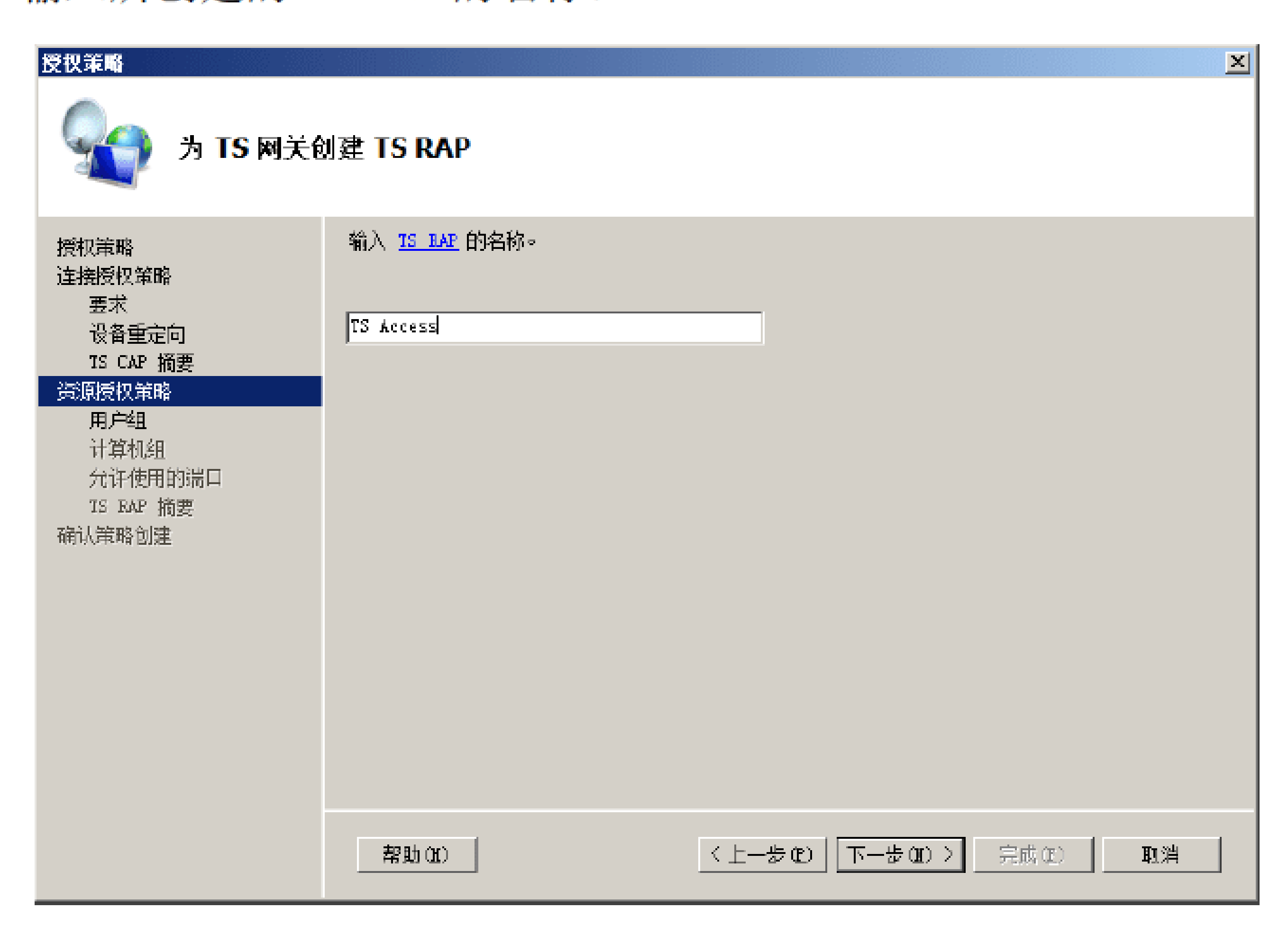


图 7-67　设置 TS RAP 名称

⑧ 单击“下一步”按钮，显示如图 7-68 所示的设置与该 TS RAP 关联的用户组对话框。这里所设置的用户组，可以通过 TS 网关远程连接到网络资源。具体添加组的操作与 TS CAP 相同，这里就不再赘述。

⑨ 单击“下一步”按钮，显示如图 7-69 所示的设置允许连接的计算机对话框。根据需要设置所允许的计算机即可，这里选择“允许用户连接到任意网络资源(计算机)”单选按钮。

⑩ 单击“下一步”按钮，显示如图 7-70 所示的设置所使用的端口对话框。默认情况下，终端服务客户端通过 TCP 端口 3389 远程连接网络资源。用户也可根据实际需要，使用其他的端口进行连接。

这里保持默认设置，即选择“仅允许通过 TCP 端口 3389 连接”单选按钮。

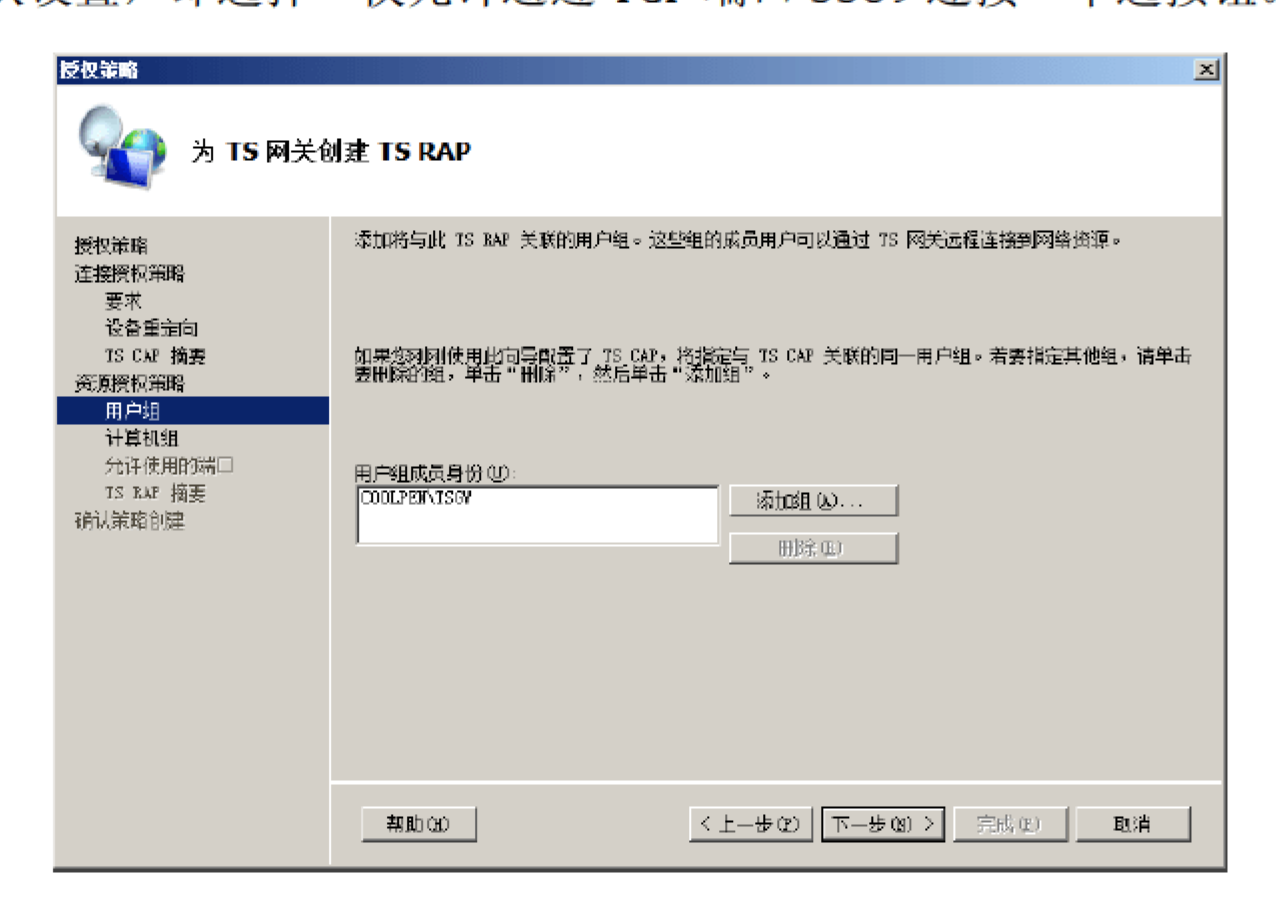


图 7-68　设置与 TS RAP 关联的用户组

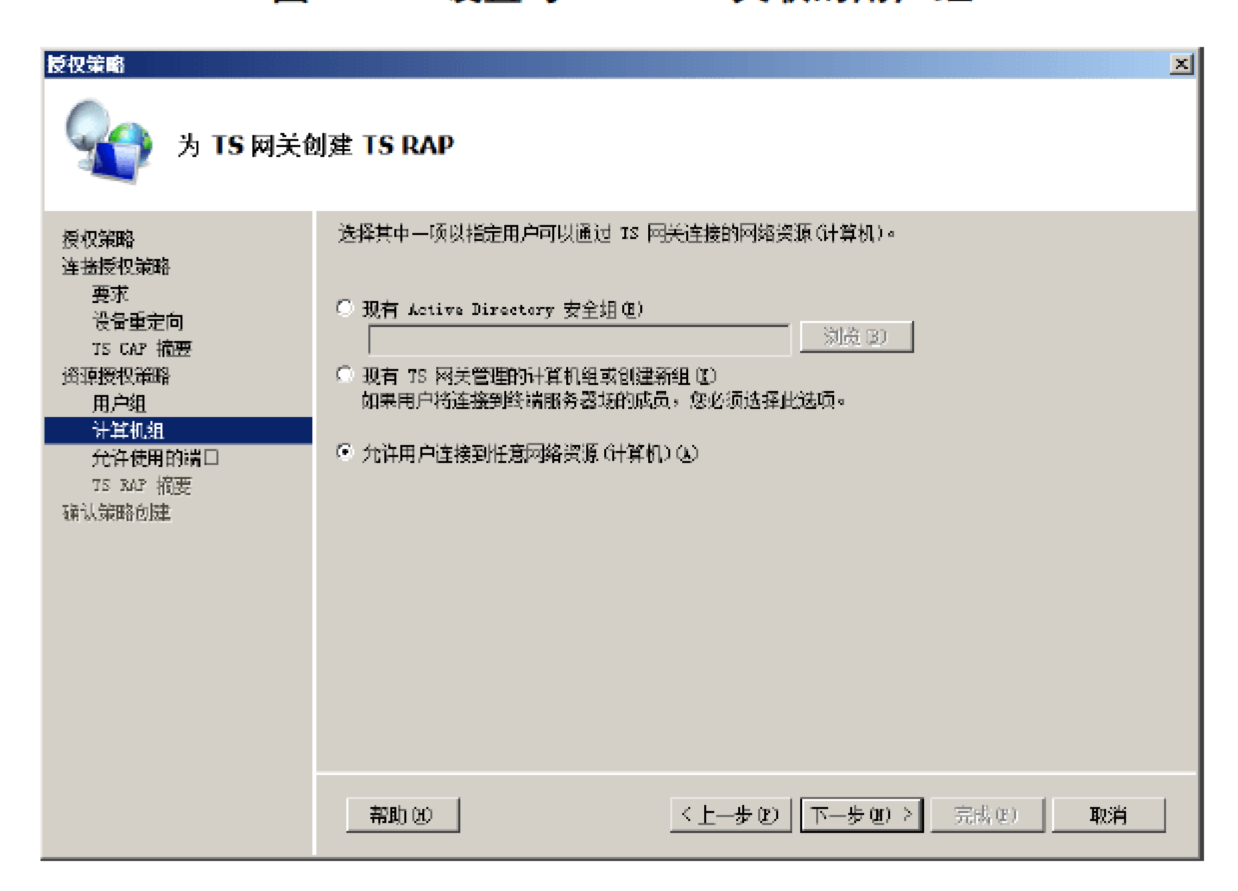


图 7-69　设置允许连接的计算机

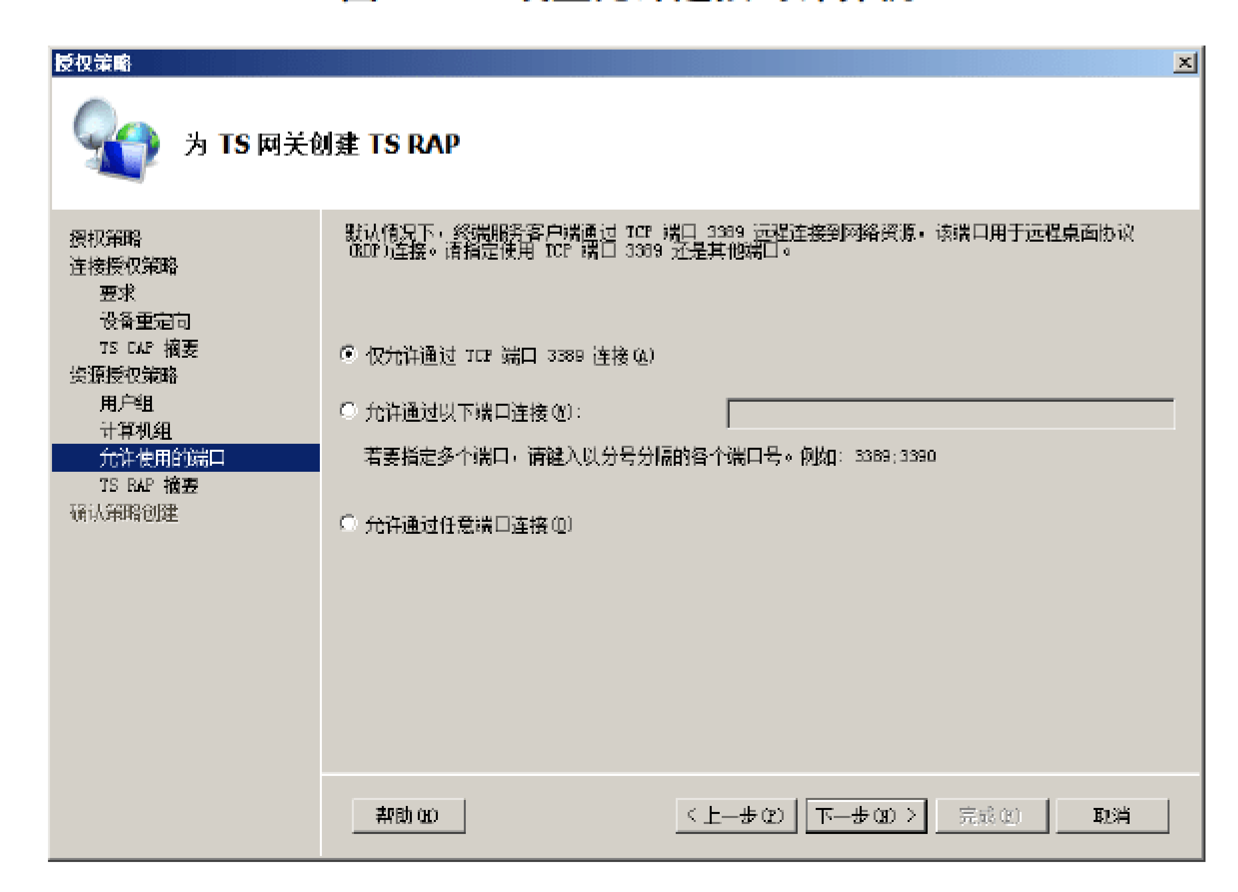


图 7-70　设置所使用的端口

⑪ 单击“下一步”按钮，显示如图 7-71 所示的“TS RAP 设置摘要”界面。检查前面的设置是否正确，单击“上一步”按钮，可以返回重新设置。

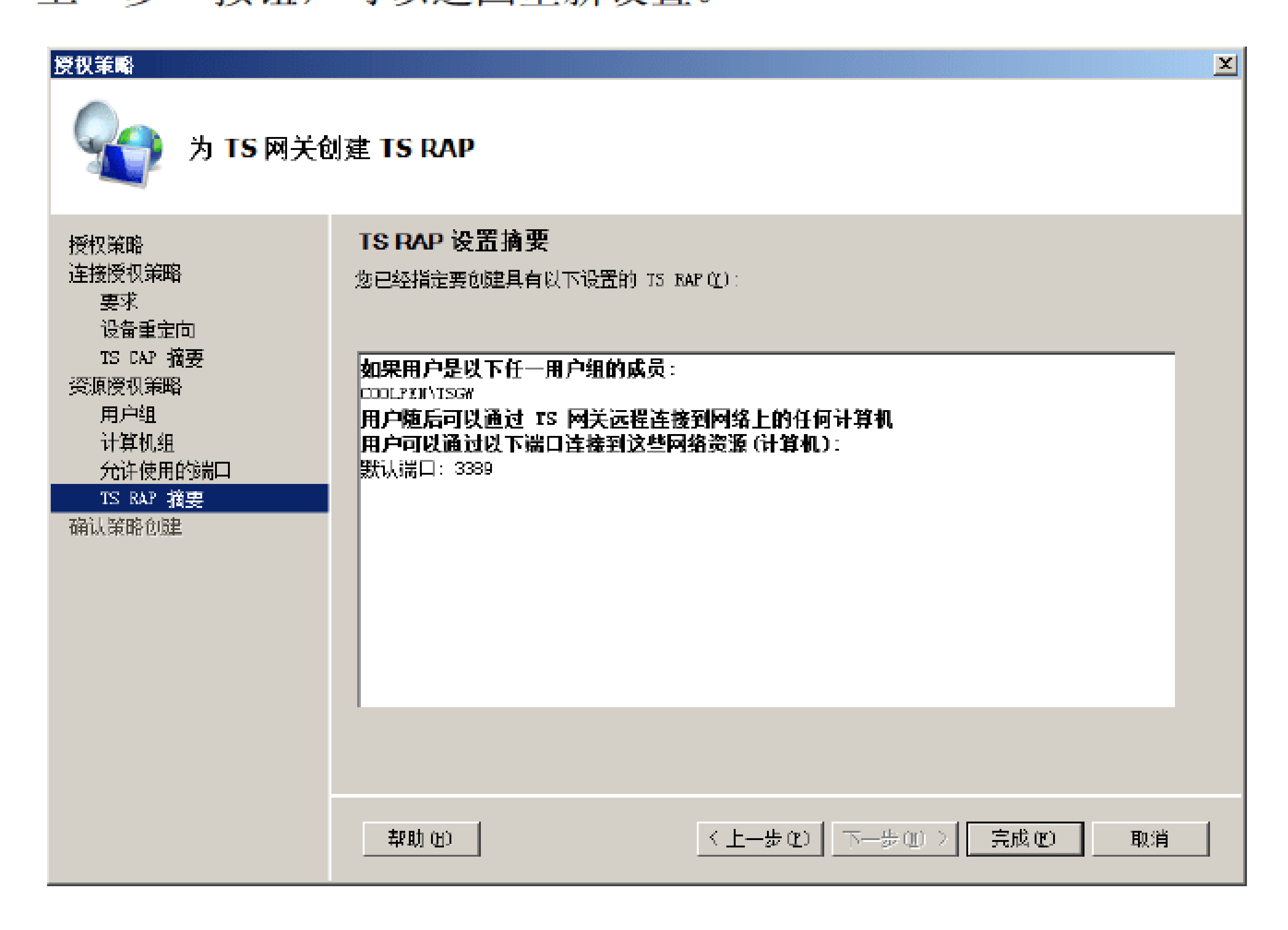


图 7-71　“TS RAP 设置摘要”界面

⑫ 单击“完成”按钮，完成终端策略的创建，显示如图 7-72 所示的“确认策略创建”界面。



图 7-72　“确认策略创建”界面

⑬ 单击“关闭”按钮，完成并关闭该向导。

7.4.5　配置终端服务客户端

终端服务客户端计算机必须验证并信任 TS 网关服务器的身份，才能安全地发送用户的密码和登录凭据，并完成身份验证过程。若要建立此信任，客户端必须信任服务器证书的根。即客户端在其受信任根证书颁发机构存储中必须有颁发服务器证书的证书颁发机构(CA)的证书。

1. 配置客户端证书

因为这里使用的是 TS 网关自创建的证书，因此，需要将该证书导入到客户端计算机中。这里以 Windows Vista 客户端为例进行介绍，具体操作步骤如下：

① 依次选择“开始”→“运行”命令，在“打开”文本框中输入 MMC，单击“确定”按钮，打开如图 7-73 所示的控制台窗口。

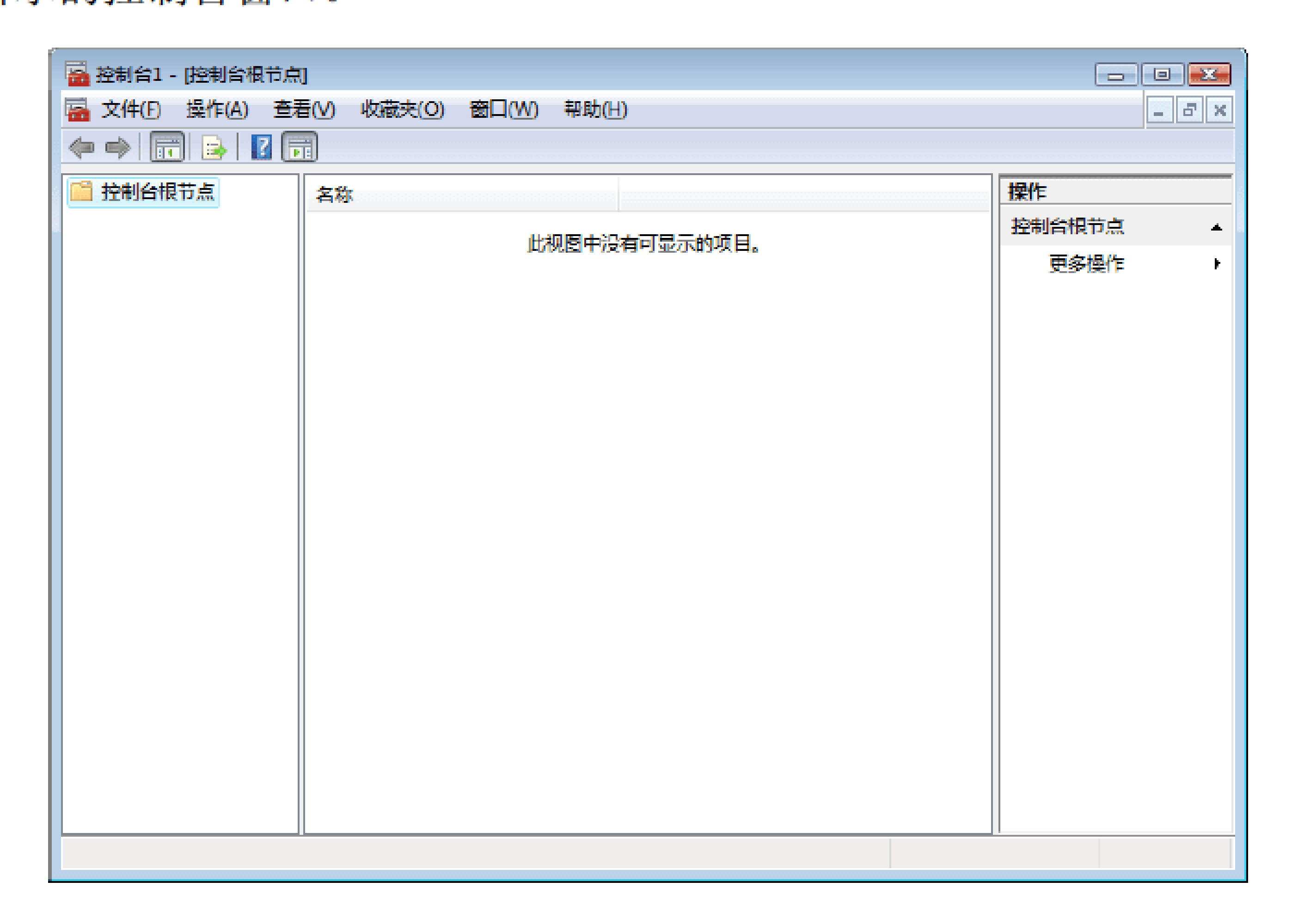
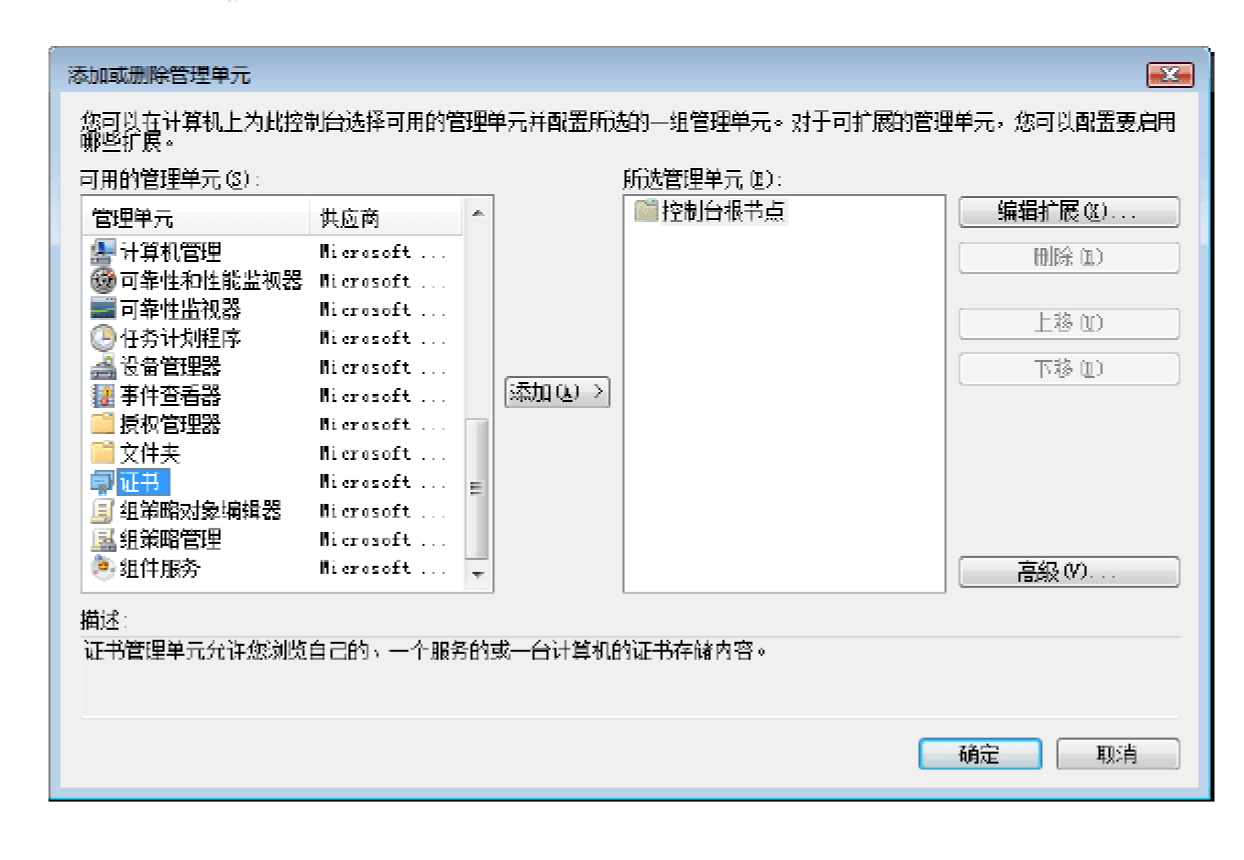


图 7-73 控制台窗口

② 依次选择“文件”→“添加/删除管理单元”命令，显示如图 7-74 所示的“添加或删除管理单元”对话框。在左侧“可用的管理单元”列表中，选择“证书”选项。

③ 单击“添加”按钮，显示如图 7-75 所示的“证书管理单元”对话框，选择“计算机账户”单选按钮。



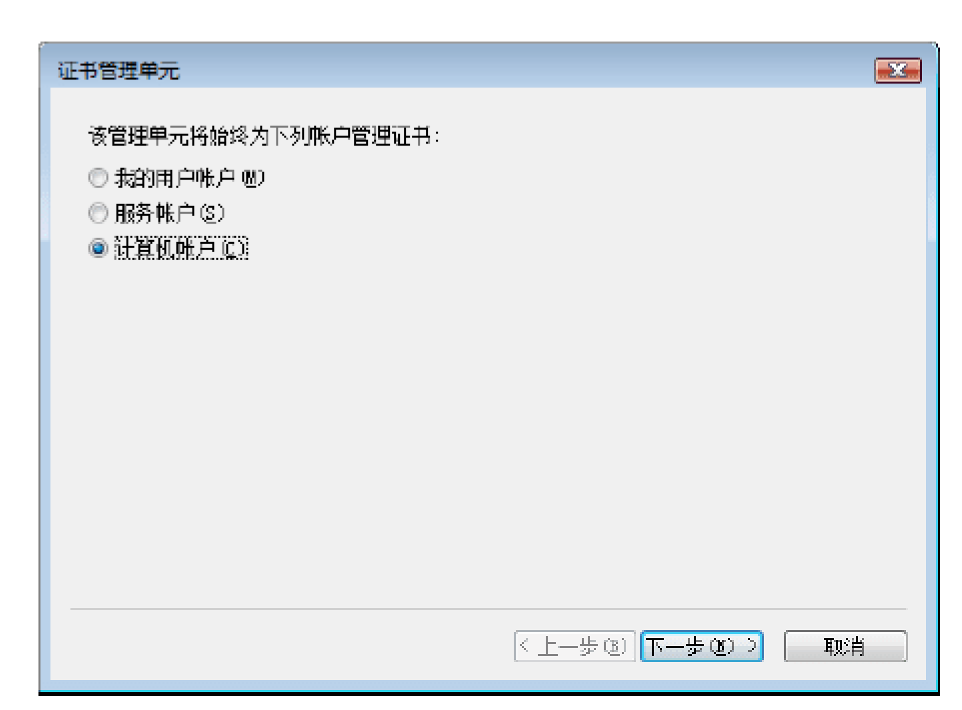


图 7-74 “添加或删除管理单元”对话框

图 7-75 “证书管理单元”对话框

④ 单击“下一步”按钮，显示如图 7-76 所示的“选择计算机”对话框，选择“本地计算机(运行这个控制台的计算机)”单选按钮。

⑤ 单击“完成”按钮，返回“添加或管理单元”对话框，单击“确定”按钮，返回“控制台”窗口，如图 7-77 所示。

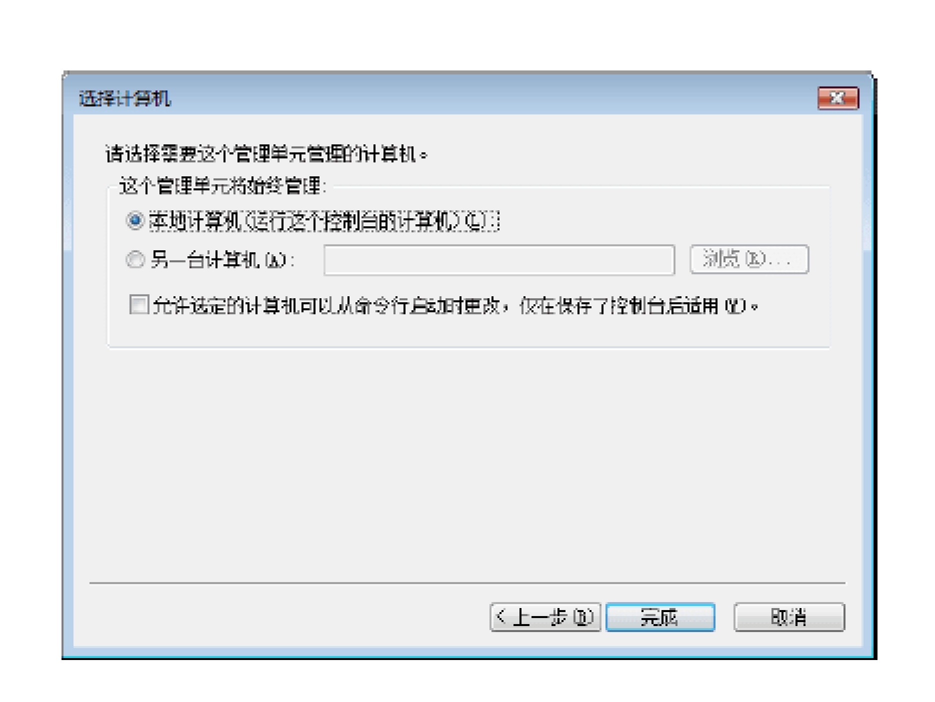


图 7-76　“选择计算机”对话框

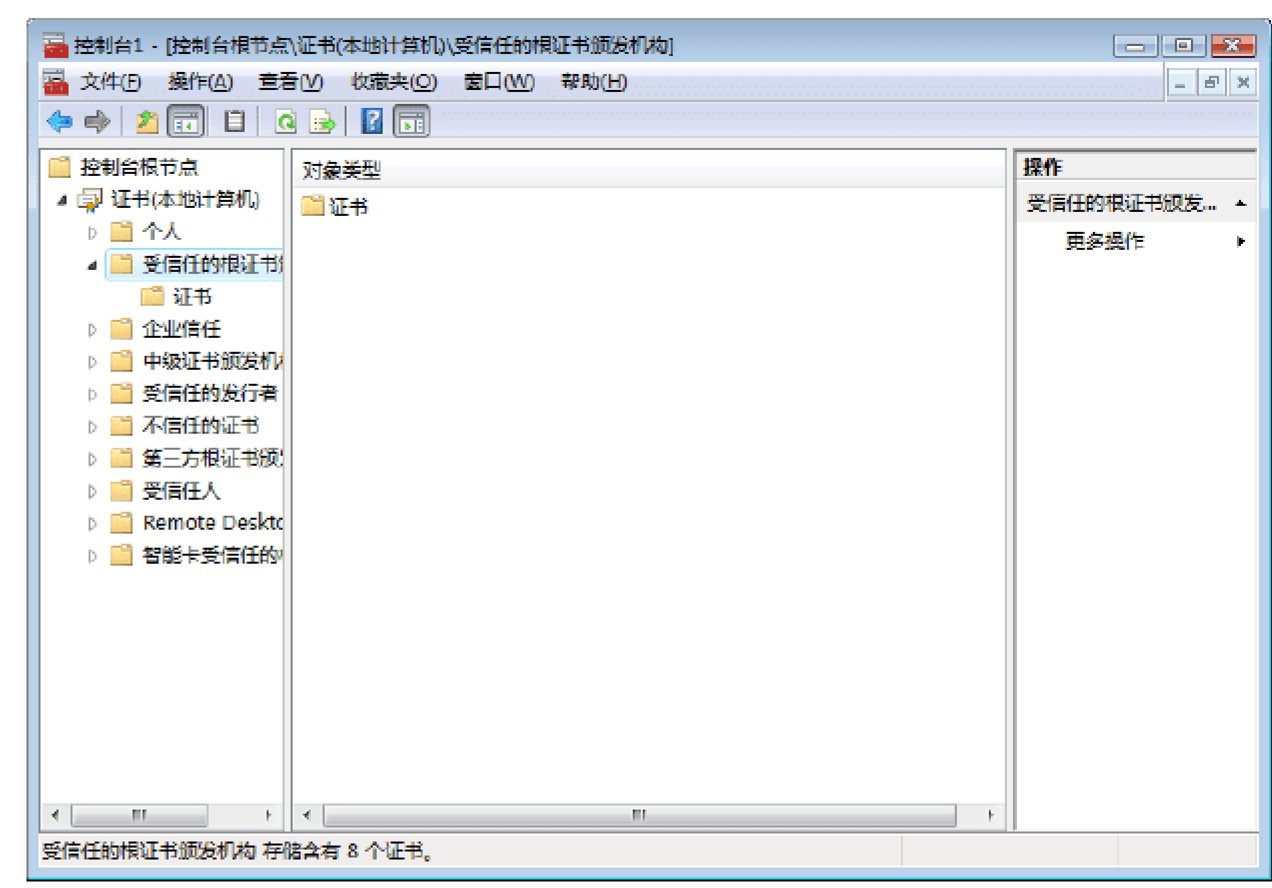


图 7-77　证书控制台

⑥ 右击“受信任的根证书颁发机构”并从快捷菜单中依次选择“所有任务”→“导入”，显示如图 7-78 所示的“欢迎使用证书导入向导”界面。

⑦ 单击“下一步”按钮，显示如图 7-79 所示的“要导入的文件”界面。在文件名“文本框”中，输入证书的目录，即终端服务器自创建的证书路径。

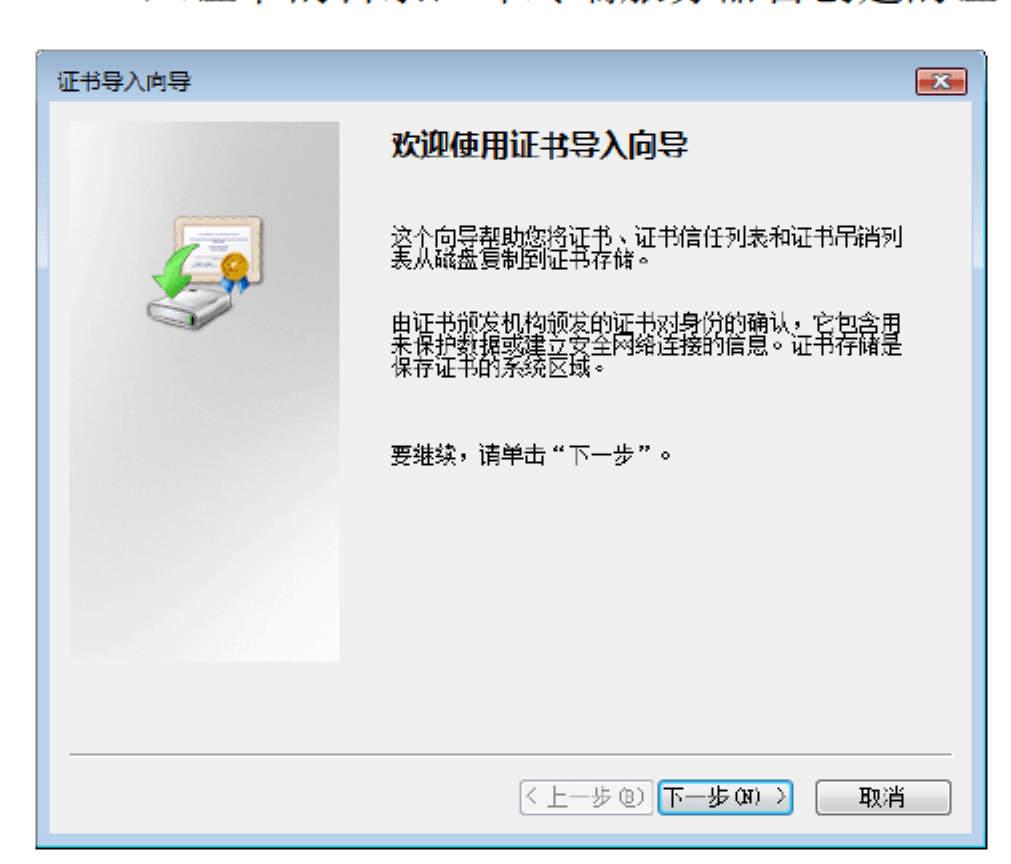


图 7-78　“欢迎使用证书导入向导”界面

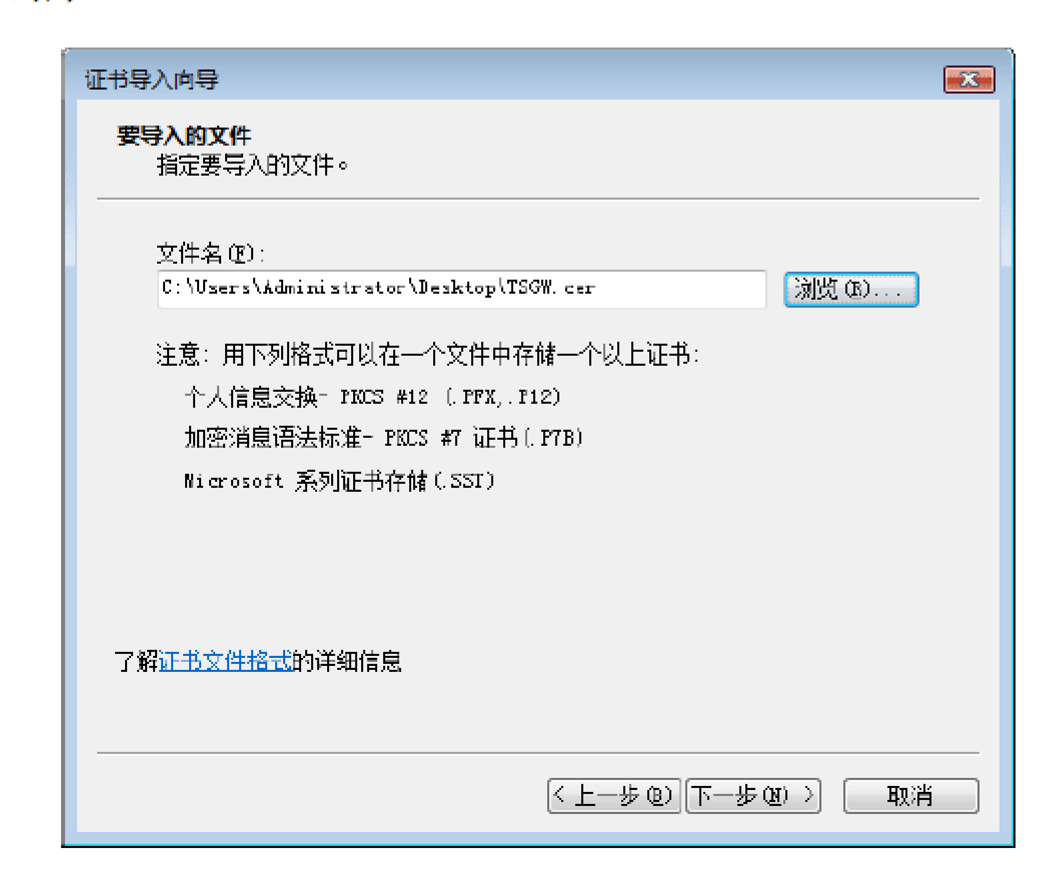


图 7-79　“要导入的文件”界面

⑧ 单击“下一步”按钮，显示如图 7-80 所示的“证书存储”界面，保持默认设置即可。

⑨ 单击“下一步”按钮，显示如图 7-81 所示的“正在完成证书导入向导”界面。

⑩ 单击“完成”按钮，确认将该证书导入到计算机中。导入成功后，显示如图 7-82 所示的导入成功提示框。

⑪ 单击“确定”按钮，完成并关闭该提示框。

2. 远程连接服务器

使用 TS 网关远程连接终端服务器，同样需要“远程桌面连接”工具。需要注意的是，远程桌面连接工具必须使用 RDP6.0，默认情况下，在 Windows XP SP3 和 Windows Vista 系统中所集成的即为 RDP6.0。

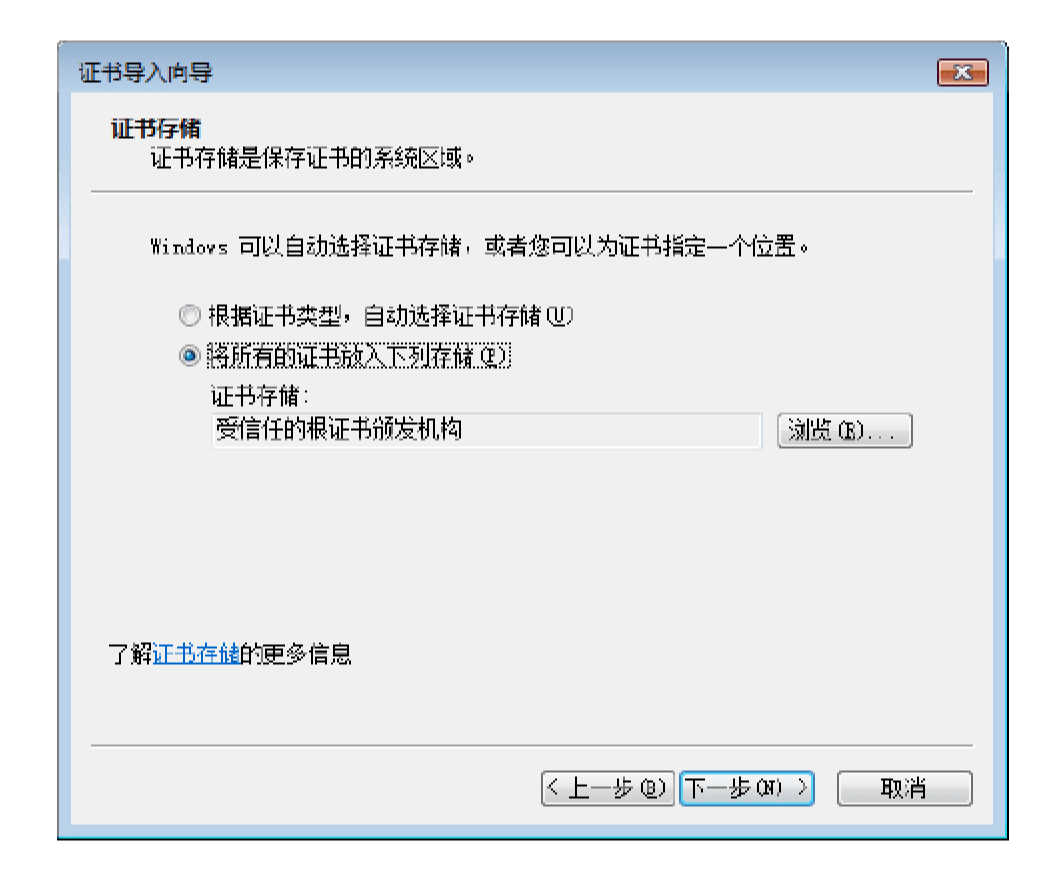


图 7-80　“证书存储”界面

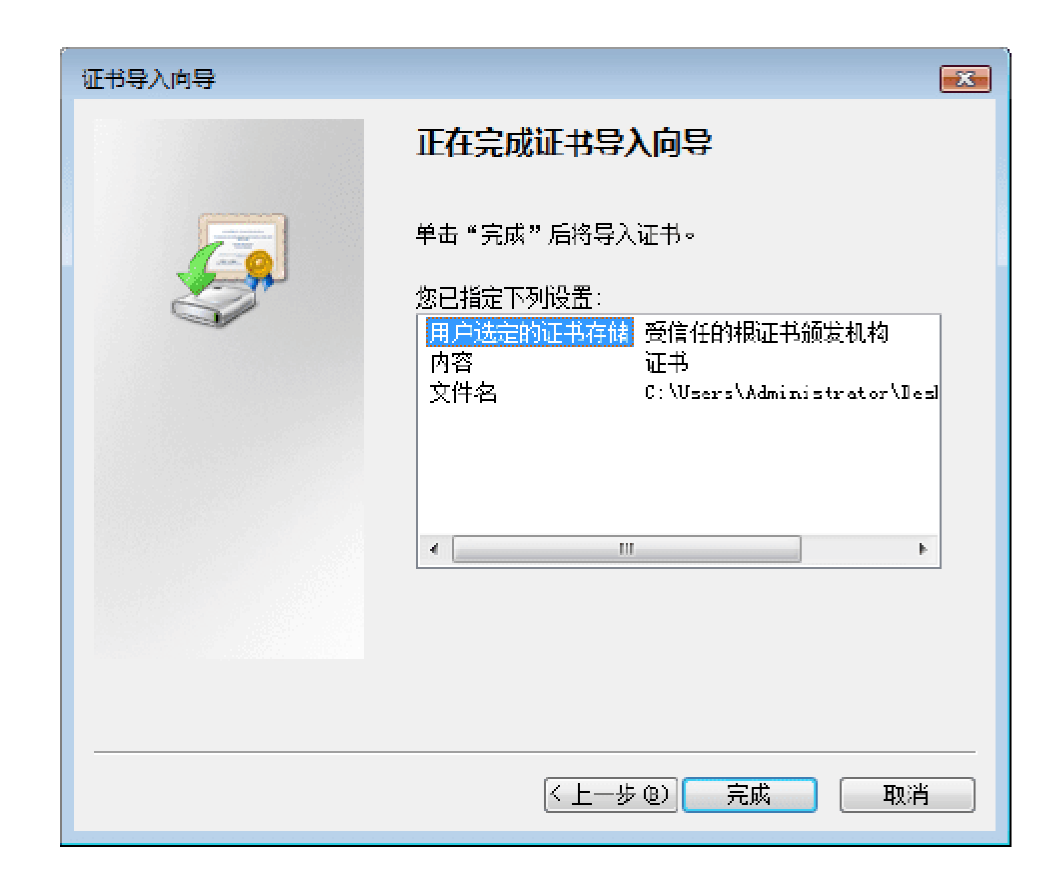


图 7-81　“正在完成证书导入向导”界面

① 依次选择“开始”→“所有程序”→“附件”→“远程桌面连接”，打开“远程桌面连接”对话框。单击“选项”按钮，设置远程桌面连接的选项，如图 7-83 所示。在“计算机”下拉列表框中，输入欲连接的终端服务器的 IP 地址。

② 其他设置与普通远程桌面连接相同，具体内容请参见相关内容，这里就不再赘述。切换到“高级”选项卡，如图 7-84 所示。

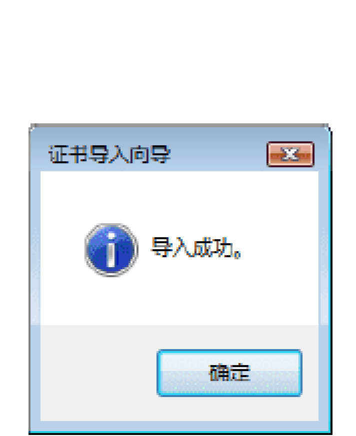


图 7-82　提示导入成功

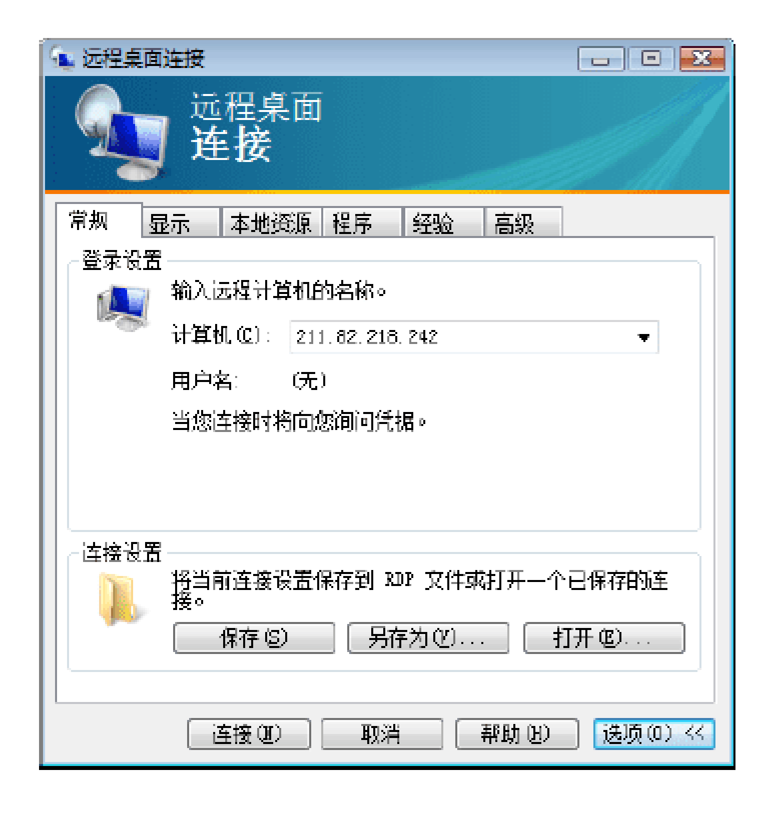


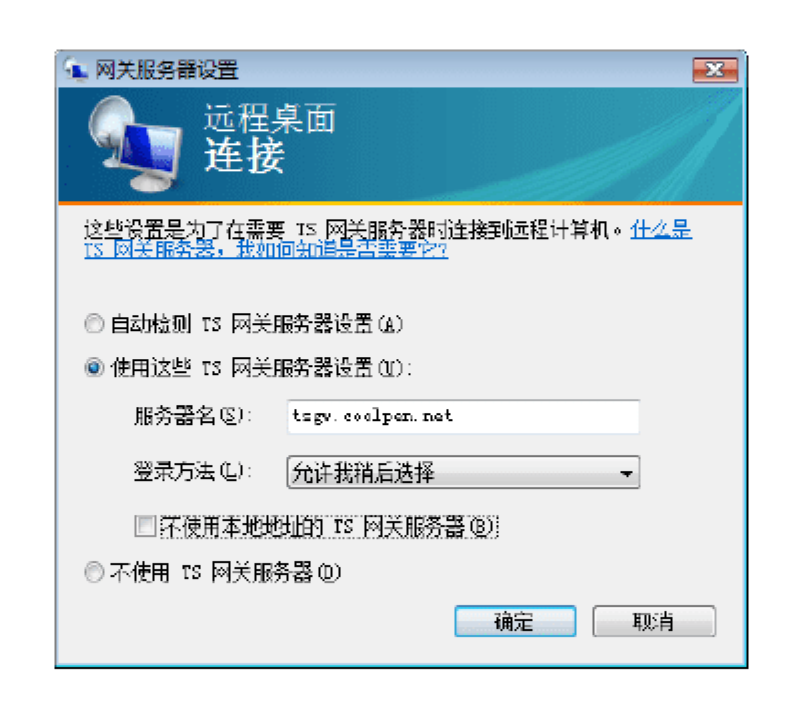
图 7-83　“常规”选项卡

图 7-84　“高级”选项卡

③ 在“从任意位置连接”选项区域中，单击“设置”按钮，显示如图 7-85 所示的“网关服务器设置”对话框。选择“使用这些 TS 网关服务器设置”单选按钮，在“服务器名”文本框中，输入网关服务器的 DNS 名称。需要注意的是，客户端计算机必须可以正确解析该名称。如果是在局域网中，为了避免不通过 TS 网关而直接连接到终端服务器，可以取消选中“不使用本地地址的 TS 网关服务器”复选框。

④ 单击“确定”按钮，返回“远程桌面连接”对话框，单击“连接”按钮，显示如图 7-86 所示的“输入您的凭据”界面。分别在用户名和密码文本框中，输入终端服务器合法的用户名和密码。这里因为终端服务器处于域环境中，因为需要输入域用户名。

⑤ 单击“确定”按钮，显示如图 7-87 所示的“网关服务器凭据”界面。分别在用户名和密码文本框中，输入网关服务器合法的用户名和密码。



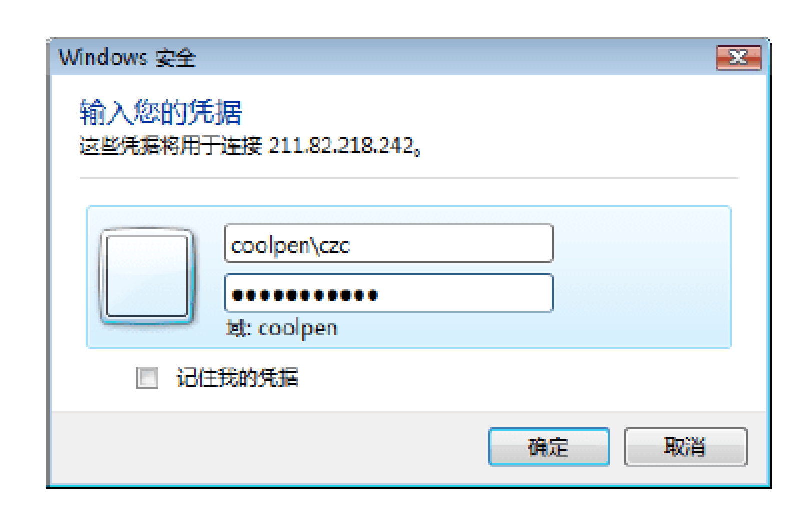
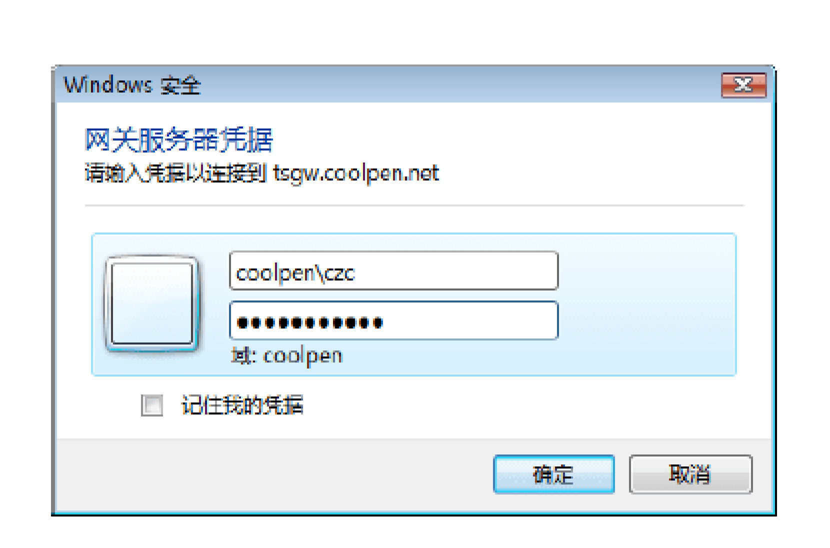


图 7-85　“网关服务器设置”对话框　　　　图 7-86　“输入您的凭据”界面

⑥　单击“确定”按钮，稍等片刻，即可成功连接终端服务器，如图 7-88 所示。



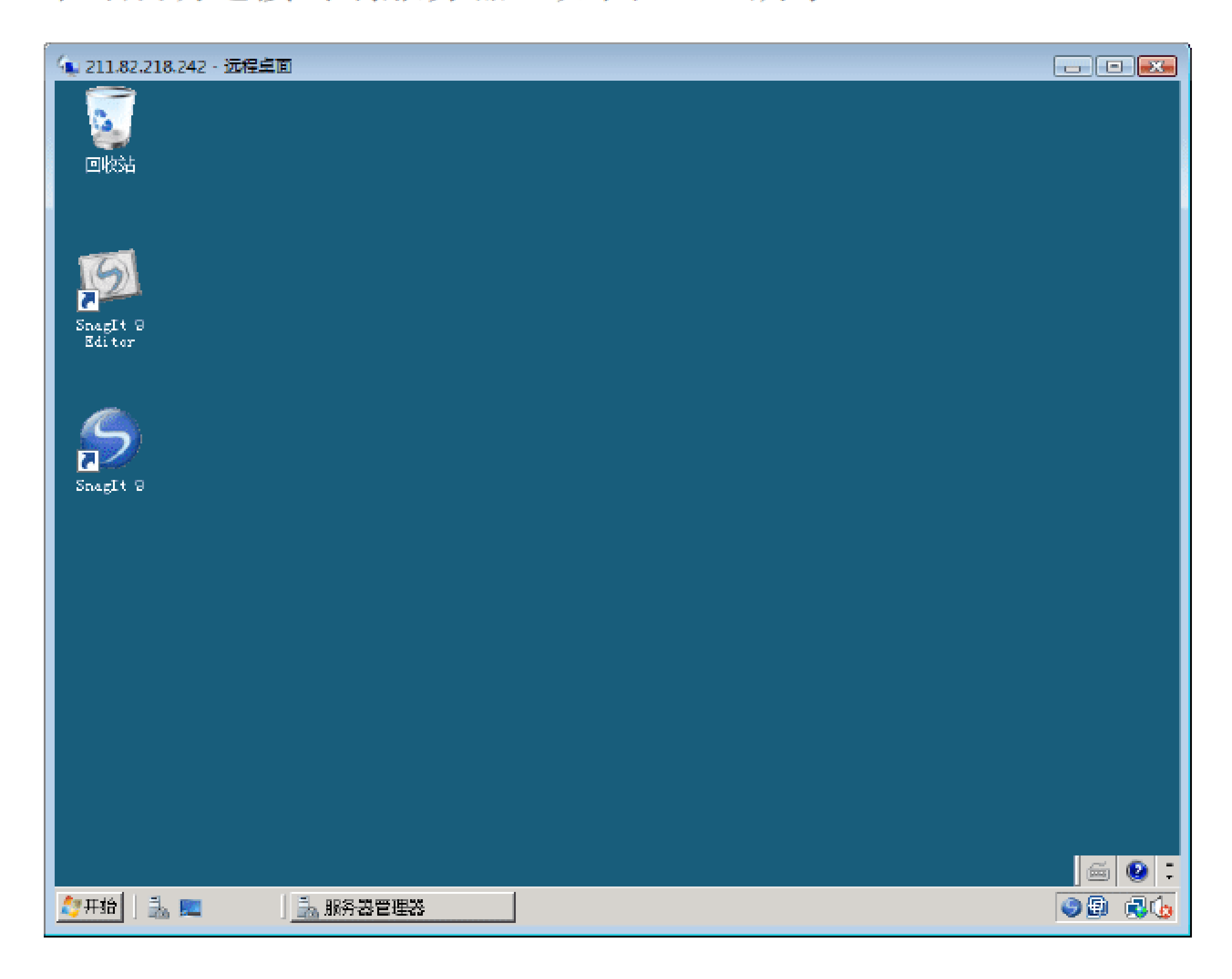


图 7-87　“网关服务器凭据”界面　　　　图 7-88　成功连接终端服务器

7.4.6　监视 TS 网关服务器的连接状态和报告

在“TS 网关管理器”窗口中，可以查看当前正在进行的连接。当发现可疑连接时，还可以断开相应的连接。

在“TS 网关管理器”窗口左侧栏中，选择“监视”选项，即可在中间“监视”栏中，显示所有正在进行的连接，如图 7-89 所示。在该窗口中，可以查看连接的 ID、用户 ID、用户名、连接在、连接时段、空闲时间、目标计算机、客户端 IP 地址和目标端口等信息。如果想要断开某个连接，可以左击该连接，在快捷菜单中选择“断开此连接”选项即可。如果在快捷菜单中，选择“断开与此用户的连接”选项，则可以断开该用户的所有连接。

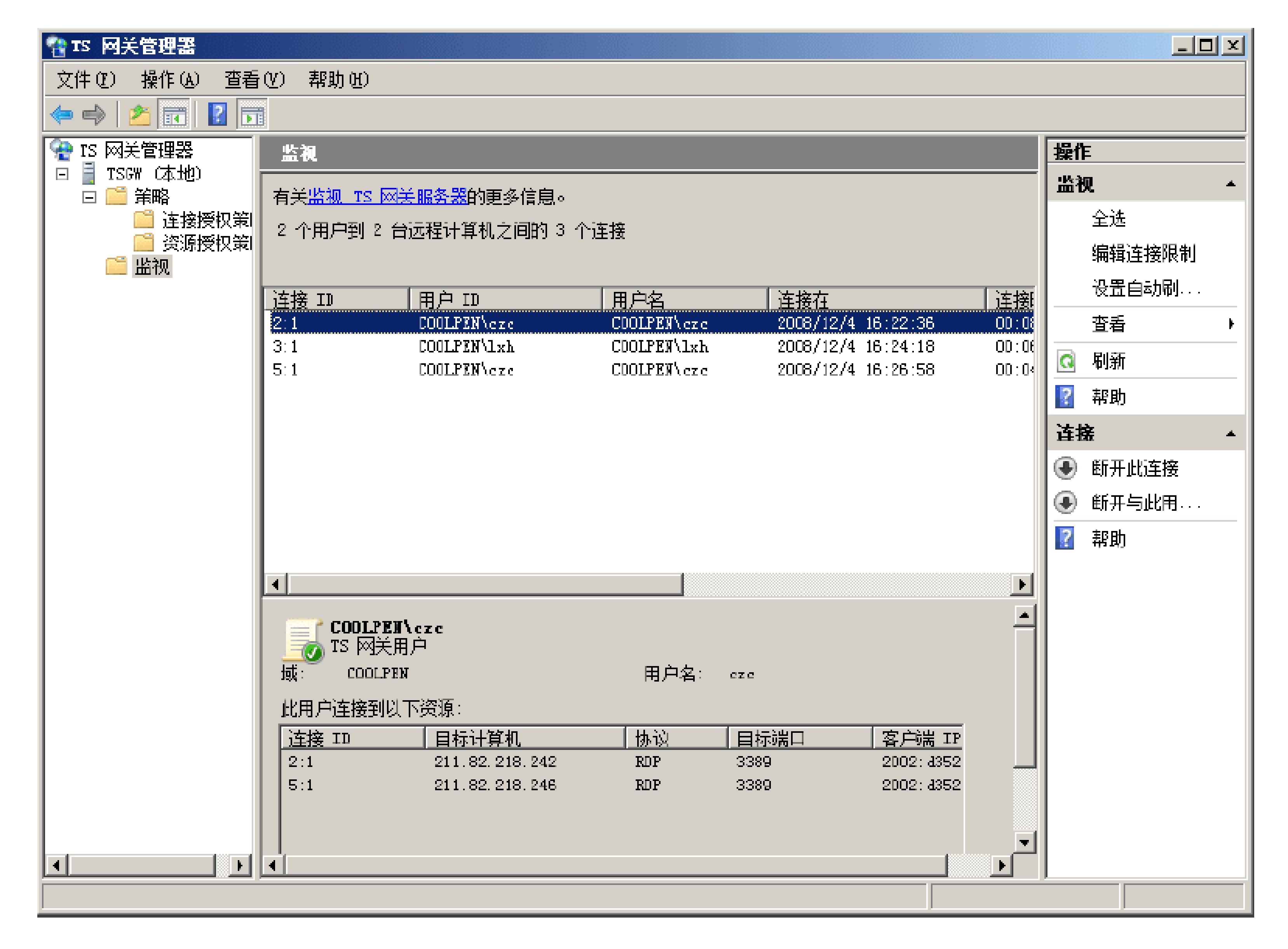


图 7-89 监视连接

7.5 文件服务安全

资源共享是网络最大的特点之一，而局域网的资源共享更多的是借助文件共享来实现。文件服务是局域网中很常用的网络服务之一，通常利用文件服务器的 RAID 卡和高速的 SCSI 硬盘为网络提供文件共享，还可以设置网络文件的保护权限，在高速存取的同时还确保了访问的安全，也能够充分利用大容量的磁盘存储空间。

在网络中，某些文件因为安全要求，只允许某些用户或组访问。此时，可以通过设置 NTFS 权限、共享文件夹权限和磁盘配额来实现。具体关于这些方面的内容请参见本书的相关章节，这里就不再赘述。

第 8 章　Windows 防火墙

Windows 防火墙是 Windows Server 2008 系统中变化较大的组件之一，它不仅是一款基于主机的状态防火墙，可以提供数据包筛选和 IP 安全(IPSec)功能，还可以帮助用户防御来自 Internet 和内部局域网的各种恶意攻击，大大提高系统安全性，是网络边界防火墙的一个有益补充。高级安全 Windows 防火墙还可以同时控制传入和传出连接，可以轻松实现端到端的安全连接和用户身份验证。

关键词

- Windows 防火墙概述
- 配置 Windows 防火墙
- 使用组策略配置 Windows 防火墙
- 配置 Windows 防火墙事件审核
- Windows 防火墙的维护

8.1 Windows 防火墙概述

最早的 Windows 系统是不集成防火墙组件的，从 Windows XP SP1 系统才开始提供，直至出现 Windows Vista/2008 之前，防护功能都比较单一，只可以阻止未通过允许的连接。一些比较复杂的网络攻击，往往需要通过监视通信或者伪装通信来实现，因此需要更加可靠的安全防护。Windows Server 2008 系统中的高级安全 Windows 防火墙，集成了 IPSec 管理，IPSec 通过双方的认证和加密来降低这种攻击的可能性。

8.1.1 使用 Windows 防火墙筛选通信

管理员可以借助 Windows 防火墙，控制哪些服务可以连接网络，哪些网络可以连接特定的服务。默认情况下，Windows 防火墙允许所有发出通信通过，但是管理员也可以限制应用程序发送通信。管理员可以创建如下形式的防火墙规则。

- 在 DNS 服务器上，只允许内部网络的请求消息。
- 在 E-mail 服务器上，允许所有计算机通过 TCP 端口 25 连接 SMTP 服务器，同时只允许内网计算机使用 TCP 端口 110 连接 POP 服务器。
- 除了 Windows 更新之外，阻止所有的应用程序和服务向外连接网络。
- 允许内网计算机对服务器使用 ping 命令，但是阻止响应来自 Internet 的 ping 请求。

8.1.2 使用 IPSec 保护通信

IPSec 是网络层提供的认证和加密安全标准，是 TCP/IP 协议的一部分。IPSec 可以有效防护探测攻击。例如，网络中的共享文件没有提供任何加密措施，攻击者通过访问物理网络就可以读取到传输中的文件内容。但是通过 IPSec 可以对网络通信进行加密，从而使攻击者基本不可能看到传输的文件内容。

1. IPSec 的身份验证功能

除了加密功能外，IPSec 还提供认证功能。通过认证功能，服务器上的 IPSec 在客户端连接之前就可以确定该客户端是否是域成员或者拥有一个有效的计算机证书。同样，客户端计算机也可以确定正确的服务器。IPSec 认证可以有效阻止常见的"中间人"攻击，如图 8-1 所示。

图 8-1　IPSec 阻止"中间人"攻击

总之，IPSec 可以阻止如下行为。

- Man-in-the-middle 攻击。
- 探测攻击。
- 重放攻击。
- 未认证的网络应用程序的访问。
- 只使用客户端 IP 地址进行认证的网络应用程序的访问。

因为 IPSec 在网络层操作，所以对于大多数应用程序来说它是透明的；但是对于有些网络设备来说 IPSec 是不兼容的。任何一个防火墙或检查通信的其他设备都不允许 IPSec 加密传输，所以用户需要经常配置这些设备来允许 IPSec 通信。

2. IPSec 的工作模式

IPSec 有两种模式：传输模式和通道模式。传输模式用来保护主机到主机的通信。在传输模式中，IPSec 通信在第 4 层传输层(OSI 参考模型)，所以 IPSec 可以加密 UDP/TCP 协议包头和原始数据，但是 IP 包头却不能被保护。通道模式用来保护主机到网络和网络到网络的通信，如 VPN。IPSec 将数据压缩到包头和包尾。按照 IPSec 协议，发送出去的数据包的原始内容将会被加密。IPSec 使用压缩安全负载(ESP)协议来提供认证和加密。如图 8-2 所示为 IPSec 的 IPv4 传输模式的数据包结构。

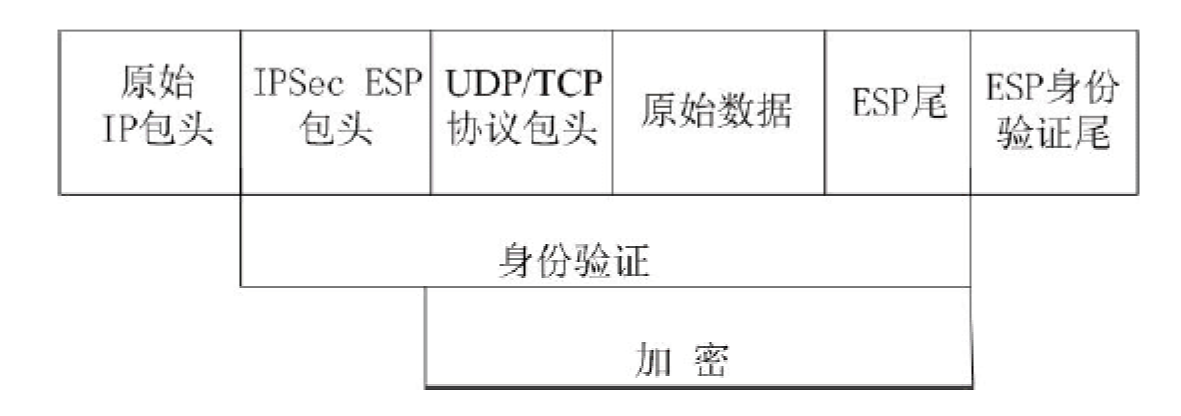


图 8-2　IPSec 数据包结构



注意：IPSec 也是 IPv6 的一部分。

应用 IPSec 加密之前需要注意的是，并不是所有的计算机都支持 IPSec。IPSec 支持多种认证和加密标准，两台支持 IPSec 的主机可能支持的是不同类型的标准。因此，在建立 IPSec 连接之前，必须确定这些主机是否都支持 IPSec 和一系列可接受的认证和加密标准。

IKE(Internet 密钥交换协议)是 Internet 安全关联和密钥管理协议(ISAKMP)和 Oakley 密钥交换协议的组合，主要用于管理在 IPSec 连接中使用的加密密钥算法。Windows Vista 和 Windows Server 2008 系统支持的 IKE 协商模式如下。

- 主模式：IKE 协商认证和加密协议，然后认证计算机。
- 用户模式：如果用户认证是为 IPSec 配置的，那么 IKE 认证用户。
- 快速模式：IKE 保护个人通信传输，并且经常改变安全密钥。但是在该模式下无法进行认证。

(1)　主模式

主模式下主要执行最初的 IKE 协商认证主机，从而产生主密钥并在机器之间建立一个 ISAKMP 安全连接，因此主模式也被称为 IKE 协商的第一阶段。默认情况下，在 Windows 系统中，ISAKMP 安全连接建立之后会保持 8 小时。如果在 8 小时后数据被转移，则主模式安全连接将会自动重新协商。

主模式协商包含下列 3 个部分。

保护序列协商。它是主模式协商的第一部分，使用无认证通信来确定可用的保护序列(其中包括加密和哈希算法、认证方法，以及 Diffie-Hellan Oakley 组)，并且决定该会话中使用的算法。IPSec 客户端会向 IPSec 服务器发送消息请求保护序列的列表，IPSec 服务器使用优先保护序列回复 IPSec 客户端的消息。

Diffie-Hellan 交换。在 IPSec 协商出保护序列之后，主模式的第二阶段就会根据 Diffie-Hellan Oakley 组协商来产生 Diffie-Hellan 公用和专有密钥对。IPSec 主机交换公用密钥，然后单独产生主模式的主密钥。该密钥将被有效应用于两台主机间的通信。

认证。主模式协商的第三阶段是执行认证。在认证过程中，基于计算机的认证优于基于用户的认证。所以当使用认证时，认证识别的是计算机，而不是使用计算机的用户。

(2) 用户模式

当主模式使用的是用户认证时，用户模式就是第二认证阶段。用户模式使用 Kerberos V5 认证活动目录中的用户账户。用户模式认证是 Windows Vista 和 Windows Server 2008 系统新引进的，所以早期版本的 Windows 系统对此不支持。

(3) 快速模式

快速模式也称第二阶段，在 IPSec 主机之间协商确立一条安全通道。在快速模式中，创建的安全连接被称为 IPSec 安全连接，连接双方均使用自己的安全参数索引(SPI)，其中一方作为信息接收端，另一方作为发送端。

默认情况下，运行 Windows 系统的计算机每小时或者每传输 100 MB 数据，就执行快速模式协商。经常使用快速模式重新协商密钥，可以降低攻击者强制破解通信密钥的可能性。

3. 认证头和 ESP

IPSec 使用如下两种协议。

- 认证头(AH)：AH 对整个 IP 数据包进行认证，但不进行数据加密，适用于某些要求严格防止 IP 欺骗的场合，所以在 NAT 模式下无法使用。
- ESP：同时提供对数据进行加密和认证，ESP 认证不对外部 IP 头进行认证，所以可以在 NAT 模式下使用。

默认情况下，Windows 系统将自动尝试使用 ESP 协议，当两台主机都不支持 ESP 协议时，才尝试使用 AH 协议。由于 ESP 协议具有广泛的支持性，AH 协议很少用到。

8.1.3 设计 Windows 防火墙策略

Windows Server 2008 系统提供的高级安全 Windows 防火墙设计非常灵活，管理员既可以对系统默认规则进行优化满足自己的需要，也可以设计和创建新的规则；并且可以为每个防火墙规则设置不同的作用范围，实现对不同访问行为的限制。当创建 IPSec 规则时，必须确定主机是否支持 IPSec，然后设计单独的策略以提供最高的安全性，保证所有客户端的连接。

1. 默认防火墙规则

默认情况下，Windows Server 2008 系统防火墙阻止所有传入通信，允许所有传出的通信，该设置可能会阻止某些网络服务的正常运行。其实，默认规则中已经包含一些常用网络服务发布规则，但默认是禁用的，管理员只需启用这些规则即可确保网络服务的正常运行。默认的防火墙策略可以满足大多数网络服务器的需要，用户也可以对如下防火墙规则进行适当编辑，实现某些特殊要求。

- 只允许来自特定子网的连接。
- 只允许来自特定用户或计算机的连接。
- 只允许受 IPSec 保护的连接。
- 只对特定的计算机应用例外。

注意： 默认情况下，Windows 防火墙允许所有传出连接，建议修改为阻止没有明确允许的连接，以便降低病毒的威胁。需要注意的是，必须确定已经为每个合法的应用程序创建了允许规则。

2. 自定义 Windows 防火墙规则

通常情况下，安装应用程序或服务组件后，将自动创建防火墙规则。例如，Windows Server 2008 系统防火墙默认规则中并未包含 Web 服务规则，但是安装 IIS 组件或其他 Web 服务器组件后，就会自动创建并启用 Web 服务规则，允许其他用户访问网站。如果应用程序没有自动创建防火墙规则，则用户可以根据如下条件手动创建。

- 程序：为某个特定的执行文件允许或阻止连接，不考虑它所使用的端口号。
- 端口：允许或阻止通过特定 TCP 或 UDP 端口号的通信，不考虑该程序产生的通信量。
- 预装 Windows 组件：例如活动目录服务、文件和打印共享服务等，虽然已经自动创建相应的默认防火墙规则，但用户也可以为其定义新的控制连接规则。
- 自定义：程序和端口两种方式结合。

由于程序规则的易配置性，用户应该首选创建程序规则。如果某项服务需要监听多个端口，需要对每个端口作不同的限制，则需要创建端口规则。

3. 控制防火墙策略作用域

所有 Windows 防火墙规则都有一个作用域，这个作用域是指允许与防火墙规定的服务进行通信的 IP 地址的范围。管理员可以根据需要编辑默认规则和自定义规则的作用域。例如，可以编辑 DNS 进入规则只允许内网访问，从而降低来自 Internet 攻击的危险。

控制进入规则作用域是避免网络攻击的有效方法之一。但是，配置作用域会增加运行管理的费用，因为每次增加子网或 IP 地址变动都需要重新配置作用域，在排除故障时必须查看规则的优先权，确定是不是应用了该规则的客户端导致的问题。

4. Windows 防火墙配置文件

防火墙配置文件是一种分组设置的方法，如防火墙规则和连接安全规则，根据计算机连接到的位置将其应用于该计算机。高级安全 Windows 防火墙中包含如下 3 种配置文件，用户可以为防火墙规则同时选定多种配置文件。

- 域配置文件：当计算机连接到本地域时应用。特别是，每当成员计算机的域控制器是可访问的时，即可应用域配置文件。
- 专有配置文件：当计算机连接专有网络时应用。默认情况下，任何网络都不是专有的，用户必须将网络标识为专有网络。
- 公用配置文件：当域控制器不可用时，默认配置文件将应用于所有网络。例如，当用户在机场或咖啡店连接 Wi-Fi 网络时，公用配置文件将被应用。默认情况下，公用配置文件允许所有出站连接，同时阻止所有的入站连接。

配置文件功能主要应用于移动计算机。当在服务器上配置规则时，通常需要为规则同时应用这 3 种配置文件。

8.2　配置 Windows 防火墙

高级安全 Windows 防火墙是 Windows Server 2008 和 Windows Vista 的新增功能之一，与标准 Windows 防火墙相比，其安全防护能力更强，具有以下特点。

- 高级安全 Windows 防火墙是双向防火墙，它不仅可以监视、设置甚至屏蔽所有的入站连接请求(默认设置为禁止)，也可以对所有的出站连接请求进行更细致的设置(默认设置为允许)。
- 高级安全 Windows 防火墙是一种基于规则的状态防火墙，支持 IPv4 与 IPv6，远比应用层级的边界防火墙更为安全。
- 高级安全 Windows 防火墙结合了主机防火墙和 IPSec；而在 Windows XP/2003 系统中，Windows 防火墙与 IPSec 是分离的。

8.2.1　配置防火墙规则

以管理员账户登录 Windows Server 2008 系统后，单击“开始”→“管理工具”→“高级安全 Windows 防火墙”命令，打开如图 8-3 所示的“高级安全 Windows 防火墙”窗口。其中包括入站规则、出站规则和连接安全规则 3 种规则。如果安装 Active Directory 服务，还会增加 13 条相应的安全规则。

- 入站规则。入站规则明确允许或者明确阻止与规则条件匹配的通信。例如，可以将规则配置为明确允许受 IPSec 保护的远程桌面通信通过防火墙，但阻止不受 IPSec 保护的远程桌面通信。默认情况下将阻止入站通信，若要允许通信，必须先创建相应的入站规则。在没有适用的入站规则的情况下，也可以对具有高级安全性的 Windows 防火墙所执行的操作(无论允许还是阻止连接)进行配置。
- 出站规则。出站规则明确允许或者明确拒绝来自与规则条件匹配的计算机的通信。例如，可以将规则配置为明确阻止出站通信通过防火墙到达某一台计算机，但允许同样的通信到达其他计算机。默认情况下允许出站通信，因此必须创建出站规则来阻止通信。

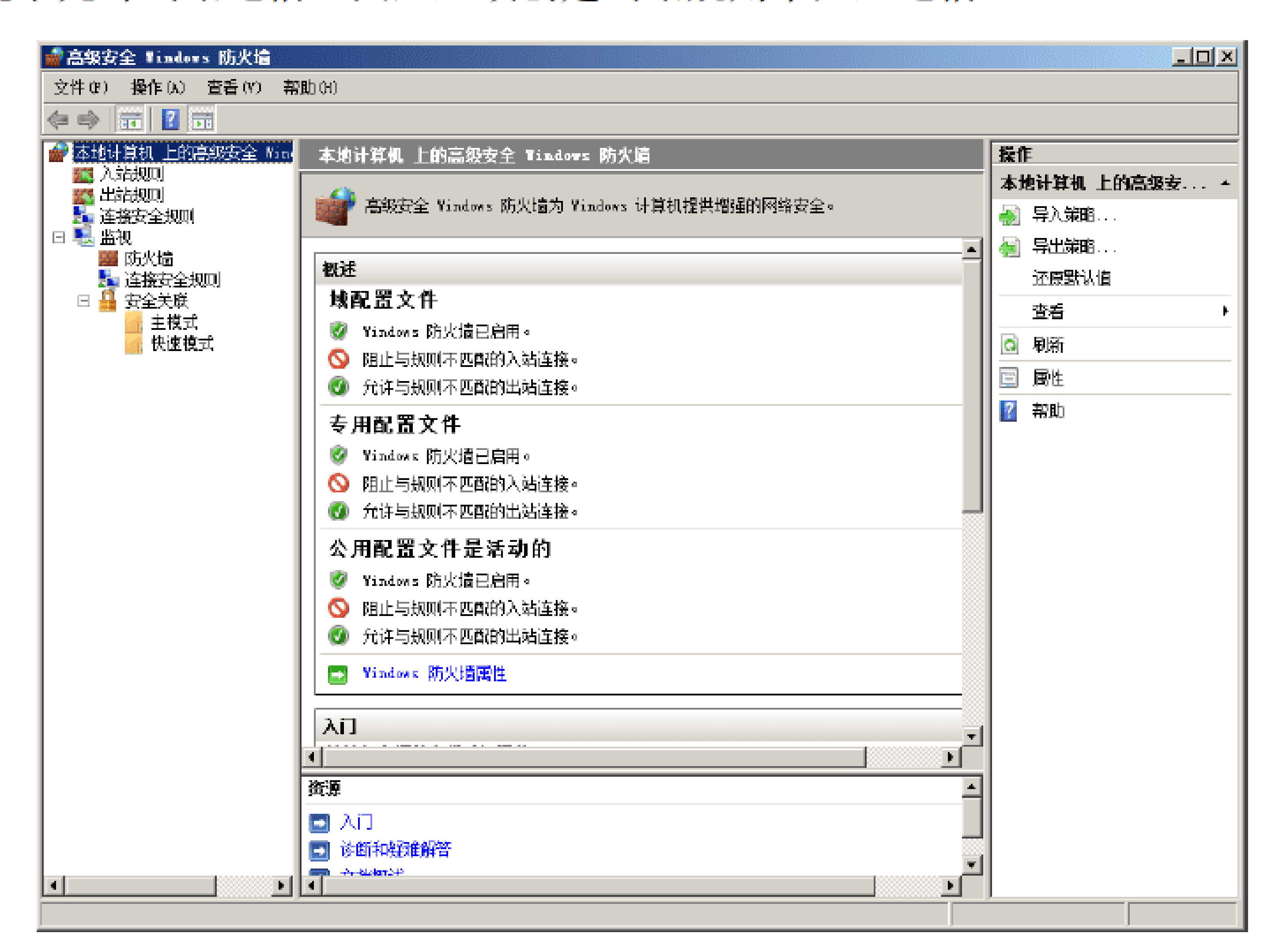


图 8-3　“高级安全 Windows 防火墙”窗口

1. 禁用或启用规则

管理员可以通过两种方式启用或禁用防火墙规则：Windows 防火墙控制台和 netsh 命令。在高级安全 Windows 防火墙控制台中，首先选择“入站规则”或“出站规则”，然后右击相应规则，从弹出的快捷菜单中选择“禁用规则”或者“启用规则”选项，即可更改其运行状态。使用 netsh 命令启用或禁用单一规则以及规则组，用法如下。

- 启用/禁用单个规则：netsh advfirewall firewall set rule name="Rule" new enable=yes | no
- 启用/禁用规则组：netsh advfirewall firewall set rule name=" RuleGroup" new enable=yes | no

例如，使用如下命令可以启用“BITS 对等缓存(RPC)”规则(默认情况是禁用的)：

```
netsh advfirewall firewall set rule name="BITS Peercaching (RPC)" new enable=yes
```

使用如下命令可以启用“BITS 对等缓存”规则组(默认情况是禁用的)：

```
netsh advfirewall firewall set rule group="BITS Peercaching" new enable=yes
```

2. 创建防火墙规则

Windows 2008 的高级安全 Windows 防火墙使用出站和入站两组规则，配置其如何响应传入和传出的请求。默认情况下，管理员在该服务器上安装微软公司提供的网络服务后，将自动添加在高级防火墙的出站规则列表中，并允许通过防火墙。但是，如果安装的是第三方网络服务，则必须通过手动创建相关规则，才可以将服务发布到网络。例如，如果在当前服务器上配置基于 Serv-U 的 FTP 服务器，必须同时创建提供上传和下载的入站规则。

① 在高级安全 Windows 防火墙控制台中，右击“入站规则”，选择快捷菜单中的“新规则”选项，打开如图 8-4 所示的“规则类型”界面。与普通 Windows 防火墙类似，同样可以通过选择应用程序、指定端口、服务等多种方式创建访问规则。这里选择“端口”单选按钮。



图 8-4　“规则类型”界面

② 单击“下一步”按钮，显示如图 8-5 所示的“协议和端口”界面。根据服务使用的协议类型选择 TCP 或者 UDP 单选按钮。本例中 FTP 服务使用的是 TCP 端口，选择 TCP 单选按钮即可。选择“特

定本地端口”单选按钮，输入服务使用的端口号，如果在配置服务器时指定了非默认端口，则在这里也应指定相应端口，例如 2121。



图 8-5 “协议和端口”界面

③ 单击“下一步”按钮，显示如图 8-6 所示的“操作”界面，选择“允许连接”单选按钮。如果选择“只允许安全连接”单选按钮，则高级防火墙只允许特定的安全用户访问服务器，即使用 IPSec 身份验证的用户。如果选择“阻止连接”单选按钮，则将阻止所有用户到服务器的连接。



图 8-6 “操作”界面

④ 单击“下一步”按钮，显示如图 8-7 所示的“配置文件”界面，设置该规则的应用范围。例如，FTP 服务器仅对 Internet 用户提供服务，则选中“公用”复选框即可，内网用户对服务器的访问将不受防火墙保护。

⑤ 单击“下一步”按钮，显示如图 8-8 所示的“名称”界面。在“名称”界面中输入该入站规则的

显示名称，便于识别。在“描述”文本框中，可以输入相关的描述信息。



图 8-7　“配置文件”界面

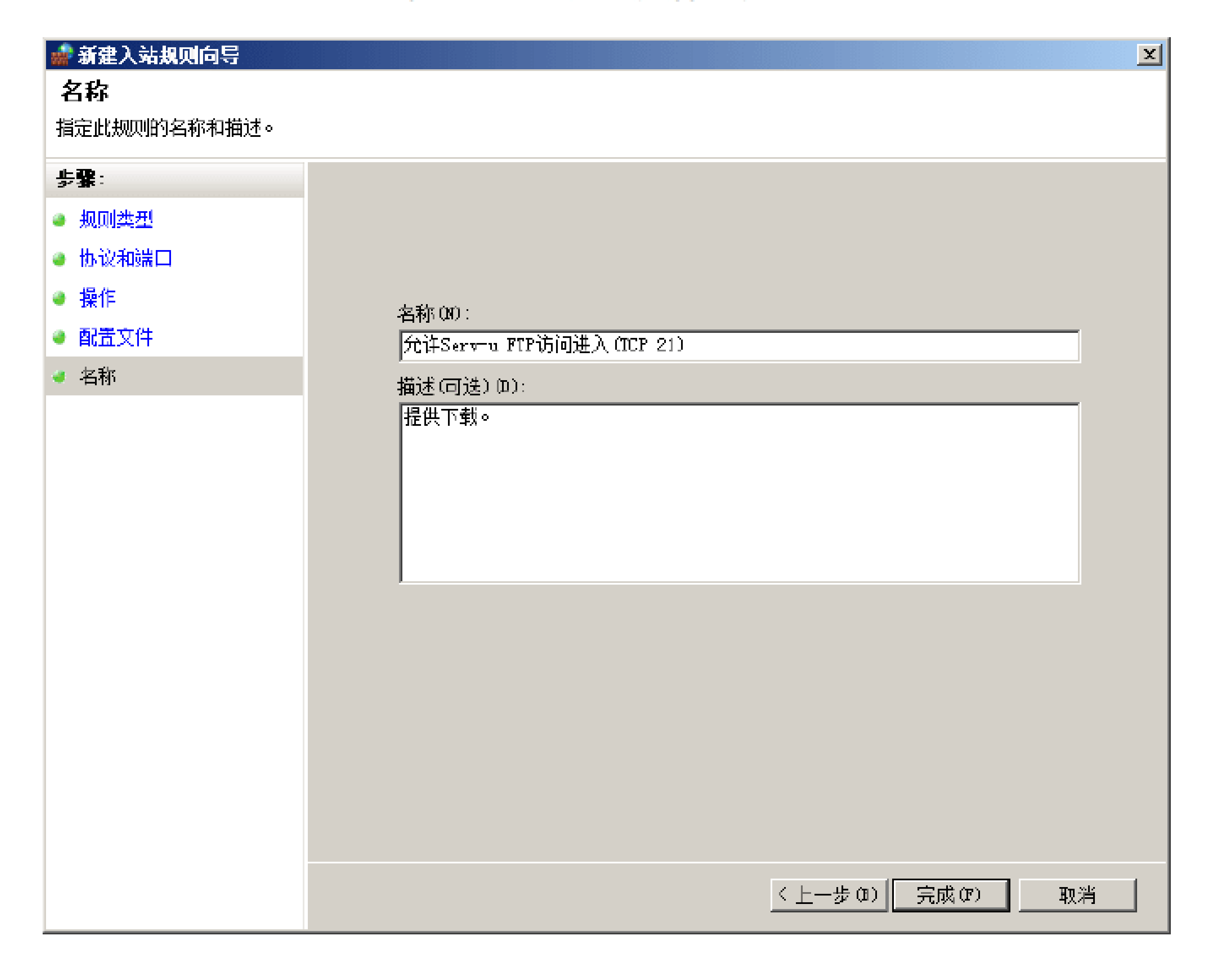


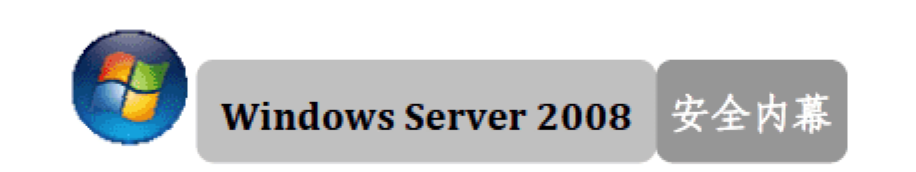
图 8-8　“名称”界面

⑥　单击“完成”按钮，即可保存已创建的入站规则。FTP 服务器提供下载和上传服务时，需要使用不同的端口，因此还需要对用于发布上传服务的端口创建入站规则，如图 8-9 所示。详细操作过程，这里不再赘述。

⑦　默认情况下，成功创建的入站规则将自动启用，并显示在“入站规则”窗口中，如图 8-10 所示。

3. 编辑防火墙规则

在 Windows Server 2003 系统防火墙中，管理员可以通过配置 ICMP 协议响应机制，使本地计算机响



应或拒绝其他计算机的 ping 入，以确保服务器安全。而在 Windows Server 2008 系统中，该协议的防火墙规则已被默认集成在高级安全 Windows 防火墙中的出站/入站规则中。用户可以通过修改配置，达到禁止响应 ping 或者禁止 ping 出的目的。

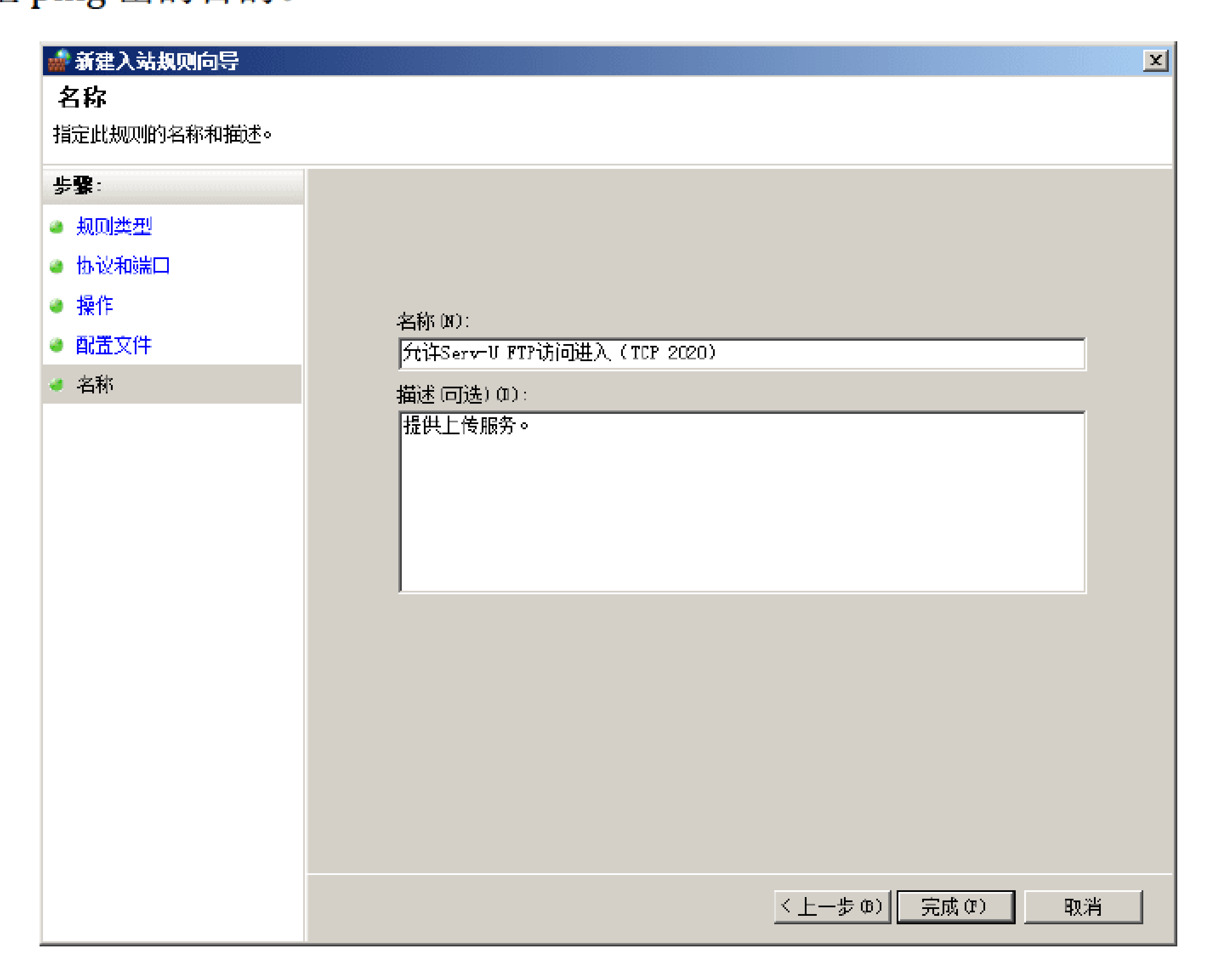


图 8-9　创建上传端口的入站规则

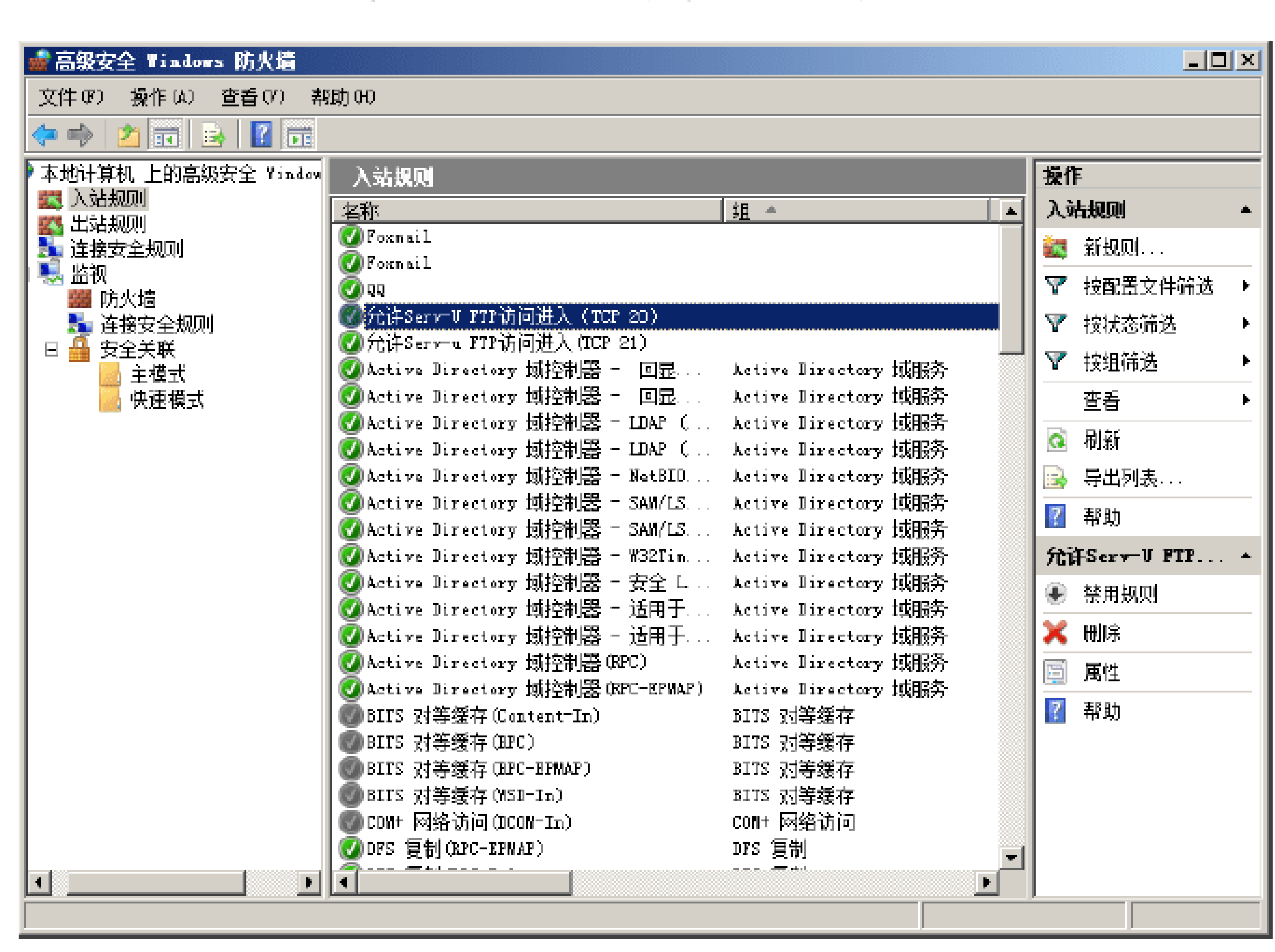


图 8-10　成功创建的入站规则

① 在高级安全 Windows 防火墙控制台中，选择“入站规则”或“出站规则”选项，右击需要配置的规则(以“网络-路由器请求”策略为例)，选择快捷菜单中的“属性”命令，打开如图 8-11 所示的“网络-路由器请求(ICMPv6-In) 属性”对话框。在“常规”选项卡中，选择“只允许安全连接”单选按钮即可启用 IPSec 保护。

② 切换到如图 8-12 所示的“作用域”选项卡，选择“下列 IP 地址”单选按钮，单击“添加”按钮，显示“IP 地址”对话框，添加指定的本地或远程 IP 地址即可。

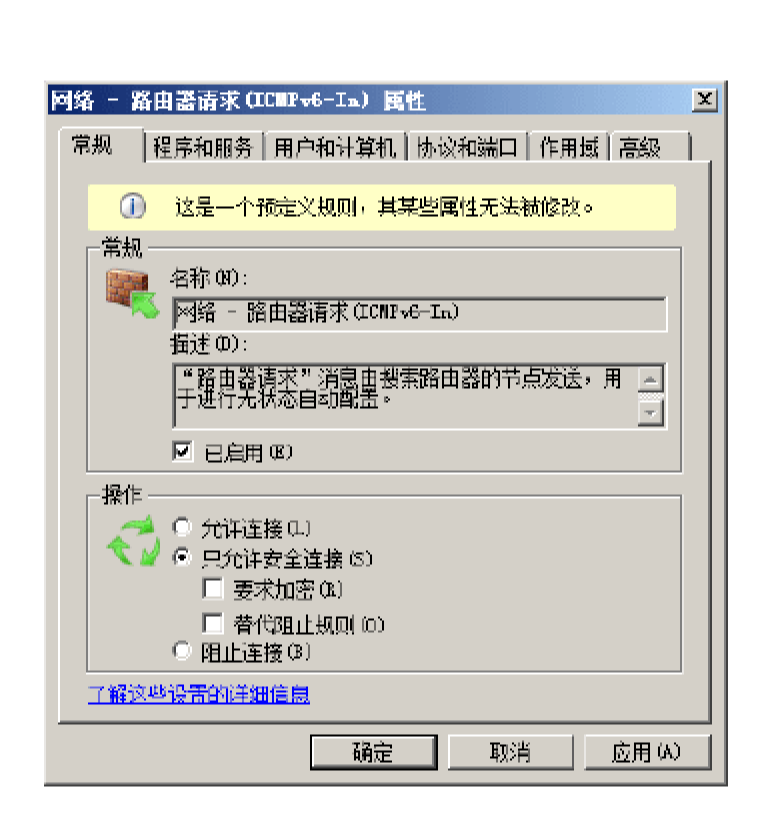


图 8-11 “网络-路由器请求(ICMPv6-In) 属性”对话框

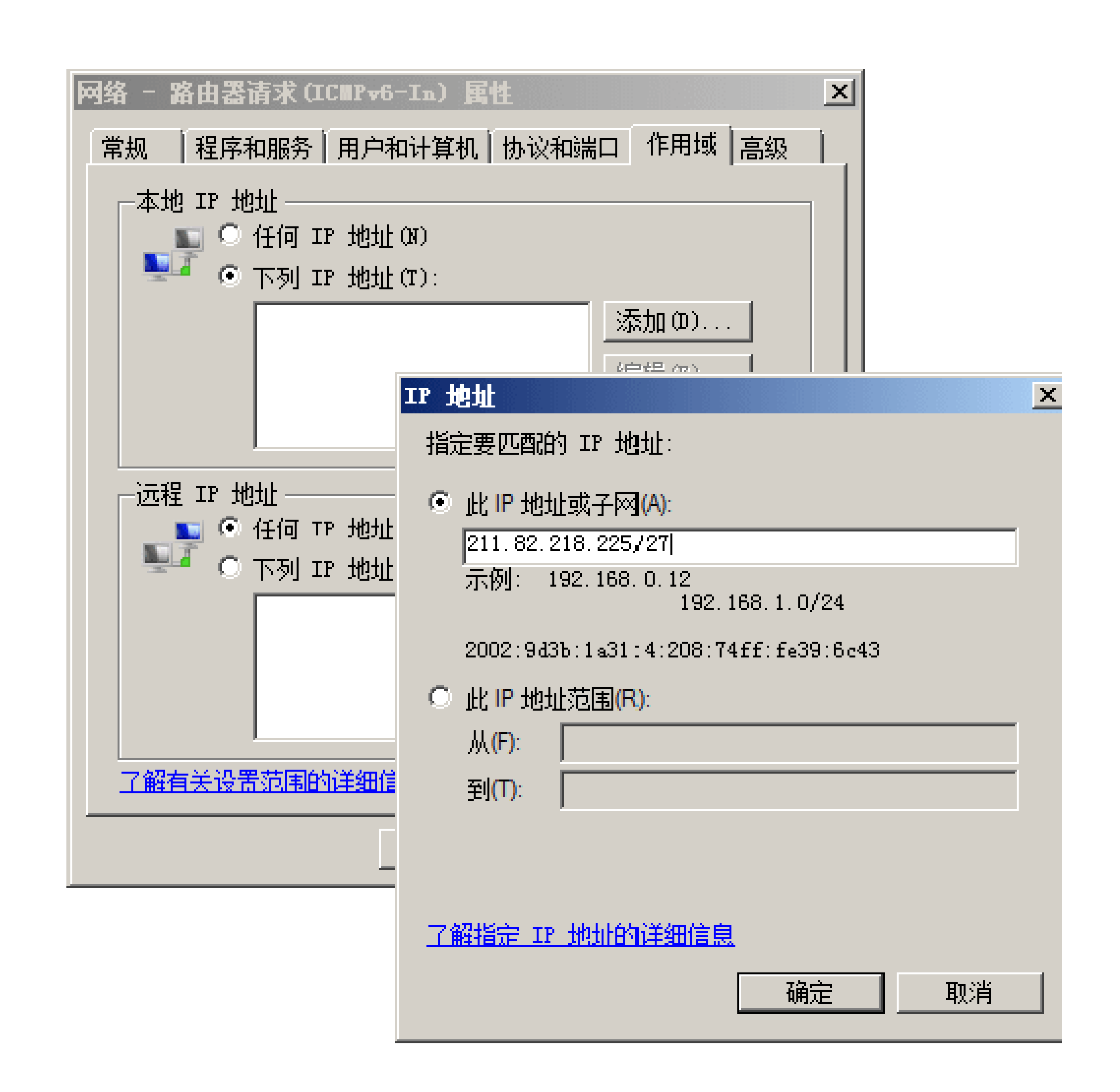


图 8-12 “作用域”选项卡

③ 切换到如图 8-13 所示的“用户和计算机”选项卡，选中“只允许来自下列计算机的连接”或“只允许来自下列用户的连接”复选框，单击“添加”按钮添加计算机或用户即可。需要注意的是，配置此选项之前，必须确保已经选择“常规”选项卡中的“只允许安全连接”单选按钮。

④ 单击“高级”标签，切换到如图 8-14 所示的“高级”选项卡，选择“下列配置文件”单选按钮，并选择需要应用规则的配置文件。

- 域：当计算机连接到其域账户所在的网络时应用。
- 专用：当计算机连接到不包括其域账户的网络时应用，例如家庭网络。专用配置文件设置应该比域配置文件设置更为严格。
- 公用：当计算机通过公用网络连接到域时应用。由于计算机所连接到的公用网络通常无法严格控制安全，因此公用配置文件设置应该最为严格。



图 8-13 “用户和计算机”选项卡

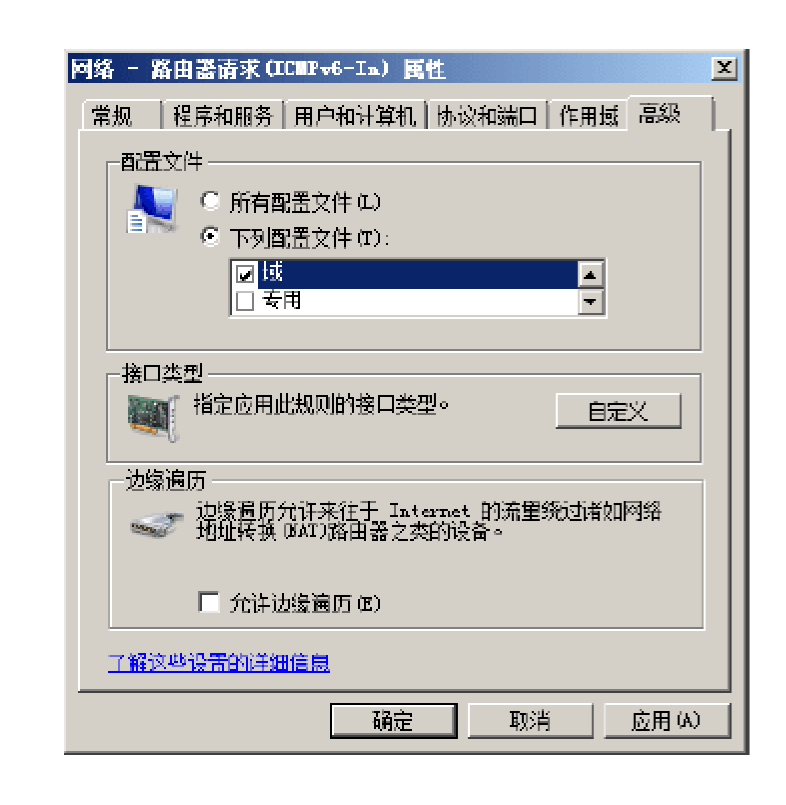


图 8-14 “高级”选项卡

⑤ 修改规则完成后，单击“确定”按钮应用并保存配置。

8.2.2 IPSec 连接安全规则

IPSec 连接安全规则允许用户为满足指定标准的连接请求 IPSec，这些标准类似于 Windows 防火墙筛选器。例如，用户可以为如下情况设置 IPSec 安全规则。

- 拒绝来自指定 IP 地址的所有通信。
- 拒绝所有来自默认网关的 ICMP 通信。
- 拒绝所有来自内网的发往指定端口的通信。
- 限制除了特定服务器的所有出站连接。

每台计算机只能拥有一个 IPSec 策略。如果多个组策略应用于一台计算机，每个组策略都有不同的 IPSec 策略，只有最高级的 IPSec 策略会起作用。

1. IPSec 规则类型

使用默认设置创建的 IPSec 规则是阻止用户通信的，即必须通过相应身份验证才可以。因此，应用之前必须确认要求认证连接的服务器和计算机，避免阻止合法用户的连接。如果环境允许，建议部署 IPSec 规则之前，在实验环境中进行测试。

管理员可以创建如下几种类型的安全规则。

- 隔离：隔离规则可根据用户定义的身份验证标准对连接进行限制。例如，可以使用此规则类型，隔离域中的计算机和域外的计算机。
- 身份验证免除：可以使用此规则类型，使特定的计算机或者指定范围内的 IP 地址(计算机)，免于对自身进行身份验证，而不考虑其他连接安全规则。
- 服务器到服务器：使用此规则类型对两台特定计算机之间、两个计算机组之间、两个子网之间，或者特定计算机和计算机组或子网之间的通信，进行身份验证。可以使用此规则对数据库服务器和业务层计算机之间，或者基础结构计算机和其他服务器之间的流量，进行身份验证。
- 隧道：如果在不支持 IPSec 的网络中，为支持 IPSec 的客户端和服务器创建 IPSec 连接安全规则，则必须使用隧道模式。这个类型的规则指定了使用隧道的主机和目的主机，以及本地和远端的网关。例如，VPN 或 IPSec L2TP 隧道等。
- 自定义：使用此规则类型创建需要特殊设置的规则。



注意：若要创建身份验证免除规则，只需要指定计算机或者一组或一个范围内的 IP 地址(计算机)并给出规则的名称和说明(可选)即可。即使对计算机免除身份验证，防火墙仍可能阻止这些计算机，除非防火墙规则已明确允许其连接。

通常情况下，隔离规则用于应用所有网络连接的策略，服务器到服务器规则用于只应用在特定网络的策略，免除认证规则用于不支持 IPSec 的计算机。

2. IPSec 认证方式

高级安全 Windows 防火墙可以提供如下几种身份验证方法。

- 默认值：选择此选项可使用“本地计算机上的高级安全 Windows 防火墙属性”对话框的“IPSec 设置”选项卡上所配置的身份验证方法。默认值中的具体参数设置如表 8-1 所示。

表 8-1　Windows Server 2008 中默认 IPSec 设置

设　置	值
认证方式	计算机(Kerberos V5)
密钥交换算法	Diffie-Hellman Group 2
数据完整性检查方法	SHA1
IPSec 认证协议	ESP
加密密钥周期	60min 或 100MB
加密方法	AES-128(主)和 3-DES(备)

- 计算机和用户(Kerberos V5)：这种方法使用计算机和用户身份验证，只允许认证域用户的计算机的连接。首先进行计算机认证，然后使用 Kerberos V5 进行用户认证来添加一层额外保护。
- 计算机(Kerberos V5)：这种方法请求或要求计算机使用 Kerberos V5 身份验证协议进行身份验证，即只允许域成员的计算机的连接。为了确保 IPSec 使用 Kerberos 认证通过受信任区域，必须使用全资格域名(FQDN)来配置信任区域。另外，还需要配置 IPSec 客户端策略，使其能够与任一域控制器进行通信，这样 IPSec 就可以从域控制器获取 Kerberos 通行证。
- 用户(Kerberos V5)：这种方法请求或要求用户使用 Kerberos V5 身份验证协议进行身份验证。
- 计算机证书：这种方法请求或要求使用有效的计算机证书进行身份验证。要使用这种方法，必须至少具有一个证书颁发机构(CA)。在使用证书认证的计算机之前，必须保证所有目标计算机都有正确的 CA 证书和相应的通行证书。此外，为了保证证书认证能预期工作，还需要在配置 IPSec 策略之前测试 PKI 基础设备。
- 高级：允许用户配置多种用户或计算机认证方式，并且指定相应的优先级。用户也可以为计算机认证使用预共享密钥，即为每个计算机配置一个密钥。因为预共享密钥在生产环境中很难改变，所以一般应用于试验环境，当任何一台计算机受到安全威胁时，就需要改变密钥。



注意：Kerberos V5 身份验证方法仅适用于 Windows 域环境，即只有计算机或用户账户是域成员时，才可以使用该验证协议。

用户可以根据需要混合使用认证方式。例如，配置公网 Web 服务器，对于内网用户可以使用 Kerberos 认证，对于外网用户可以使用公用密钥证书进行认证。在配置完 IPSec 之后，需要比较远程主机的 IP 地址和 IPSec 策略，然后决定使用哪种认证方式。

在使用 IPSec 之后，客户端就可以创建一条通向服务器的网络连接了。但是应用程序可能也需要认证。例如，某个认证用户连接到一个需要认证的文件服务器上，当客户端尝试连接共享文件夹时，可能仍然需要认证。如图 8-15 所示为 IPSec 规则网络通信中的位置和作用示意图。

3. 服务器和域隔离

“隔离”最初只是一种网络结构技术，即将计算机置于单独的物理网络中，使外网无法访问，从而阻止未经认证的用户访问网络中的计算机。IPSec 认证能够提供高可靠性的逻辑隔离，该方式允许客户端连接各种网络。服务器和域隔离只允许认证用户建立网络连接。认证发生在网络层，从而有效地保护网络通信。另外，IPSec 还会加密受保护的通信，防止攻击者通过物理网络截获数据。

- 域隔离：只有域成员才能建立网络连接。

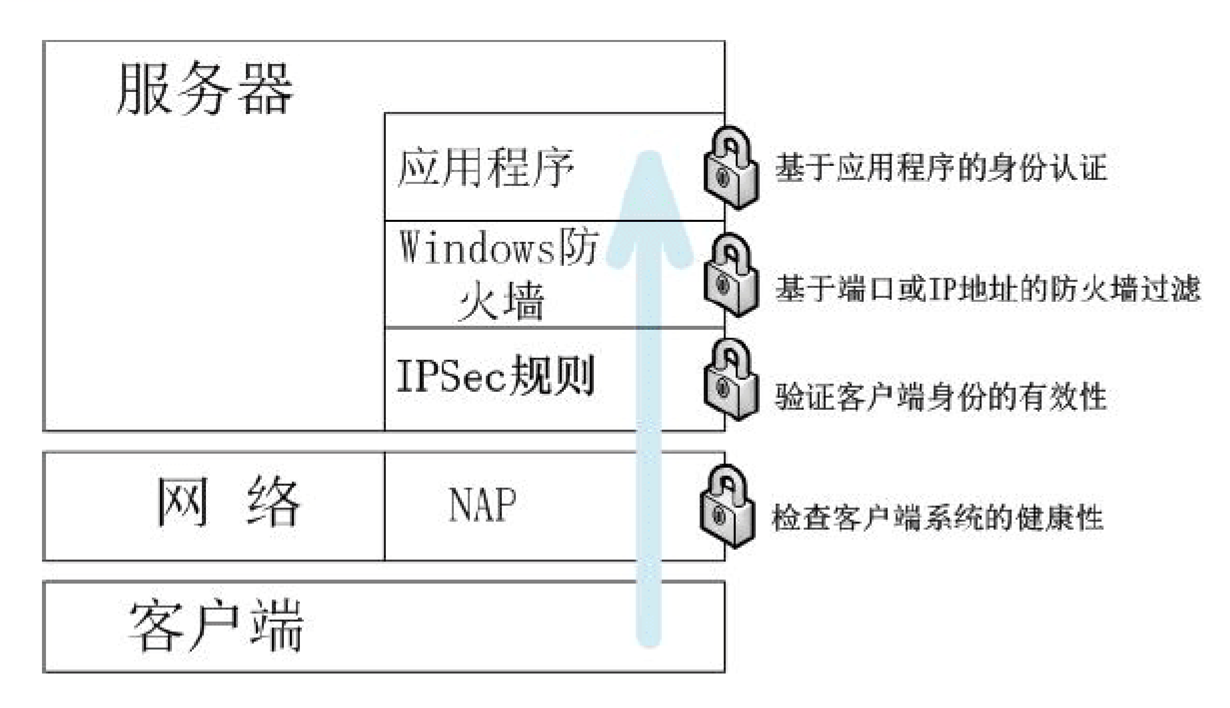


图 8-15 IPSec 在网络通信中的位置和作用

- 服务器隔离：指定服务器只接受来自受信任域成员或特定组的域成员的网络连接。服务器隔离还可以为那些不是域成员的计算机提供连接，但是必须要有受信任 CA 颁发的计算机证书。

服务器和域隔离可以有效降低如下风险。

- 连接不受保护的无线网络和访问不要求应用层认证的服务器。
- 允许任何用户(包括物理连接网络)访问的服务器。
- 使用未认证计算机连接的认证用户。

服务器和域隔离只是安全性中的一层，不能防止如下危险。

- 认证用户使用了误用访问的认证计算机。
- 访问认证计算机的攻击者。
- 攻击认证计算机和其他网络计算机的蠕虫等病毒。
- 攻击者访问不受 IPSec 保护的服务器。
- 满足 IPSec 免除的未授权连接。

4. IPSec 免除

在 Windows Server 2008 中默认情况下不要求 IPSec 认证，用户只有需要 IPSec 通信时才会需要 IPSec 免除。如果用户需要使用 IPSec 认证，则需要为不支持 IPSec 认证的连接创建 IPSec 免除。通常情况下，管理员需要为如下用户创建 IPSec 免除。

- 最新配置的计算机，还没有对 IPSec 进行配置。
- 操作系统不支持 IPSec。
- Gutst 账户。

应尽量减小免除的范围，通常只对不支持 IPSec 认证的连接批准免除。例如，管理员可以在来宾无线接入上为某主机添加免除，使其能够连接代理服务器和访问 Internet。很多基础服务器都需要使用 IPSec 免除。

- DHCP 服务器：DHCP 服务器需要通过 UDP 端口 68 来接收 DHCP 协商通信，但是不需要 IPSec。
- DNS 服务器：为允许客户端查找域控制器和其他网络资源，DNS 服务器必须允许 DNS 请求不使用 IPSec 通过 UDP 端口 53。
- Windows Internet 名称服务(WINS)服务器：如果客户端计算机需要 WINS 服务器，则需要为 WINS 请求所使用的 UDP 端口 137 创建一个免除。
- 域控制器：域控制器必须能够接受几种不受 IPSec 保护的、不同的通信协议的连接。

每个创建的免除都是一个安全风险，必须仔细评估每个免除，然后采取措施降低安全风险。应考虑攻击者使用免除访问受保护资源的所有可能性。例如，如果允许未经认证来宾用户访问代理服务器，就要确定该用户不能使用代理服务器访问其他受保护的资源，如内部文件服务器、FTP 服务器等。

另外，用户还应该使用物理访问和网络访问保护(NAP)来保护使用免除的网络。例如，如果需要为一台新配置的计算机创建一个免除，那么可以使用物理锁来限制网络访问。这将防止受 IPSec 保护的计算机去访问那些允许不受 IPSec 保护计算机访问的资源；可以降低机密信息突然外泄给未认证计算机的危险，以及降低来自未认证计算机的病毒攻击内网计算机的危险。

最后，还需要应用深度防御安全法则，不能仅依靠 IPSec 的安全性。如果内网的 Web 服务器需要 IPSec，那么用户还需要在 Web 应用程序中使用认证。同样，如果使用 IPSec 加密 E-mail 服务器的通信，则还需要启动应用层加密(例如，SSL 证书加密)。

如图 8-16 所示为 IPSec 连接策略在网络中的基本部署。域隔离应该用于限制连接到域成员的 IPSec 连接。

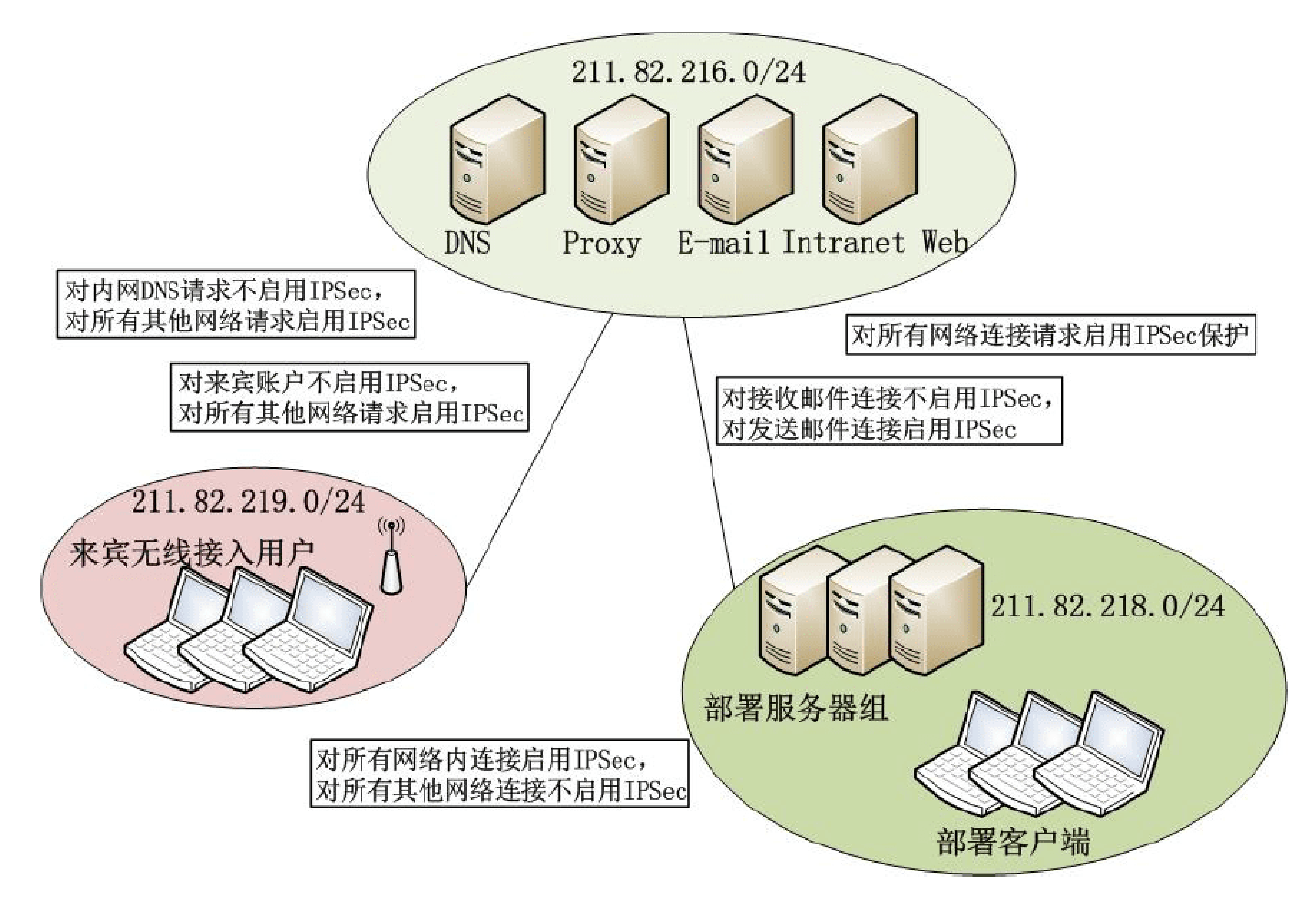


图 8-16　使用免除的隔离示例

5. 创建 IPSec 规则

① 打开“高级安全 Windows 防火墙”窗口，右击“连接安全规则”，选择快捷菜单中的“新规则”命令，启动“新建连接安全规则向导”，默认显示如图 8-17 所示的“规则类型”界面。

② 选择“自定义”单选按钮，单击“下一步”按钮，显示如图 8-18 所示的“终结点”界面。终结点是形成对等端连接的计算机或计算机组，可以是指定的单个计算机，也可以是一个本地子网。选择“下列 IP 地址”单选按钮，单击“添加”按钮，即可添加终结点计算机。

③ 单击“下一步”按钮，显示如图 8-19 所示的“要求”界面，为出站和入站连接选择是否需进行身份验证。身份验证并不能提供很好的安全性，因为恶意攻击者会选择不需要认证，但是它可以将所有不支持 IPSec 或没有证书的连接都退回。当所有合法客户端都支持 IPSec 时，可以为入站连

接选择要求安全认证；当所有服务器都支持 IPSec 时，可以为出站连接选择要求安全认证。本例中选择“入站和出站连接请求身份验证”单选按钮。高级安全 Windows 防火墙可以提供如下几种身份验证要求。



图 8-17 “规则类型”界面

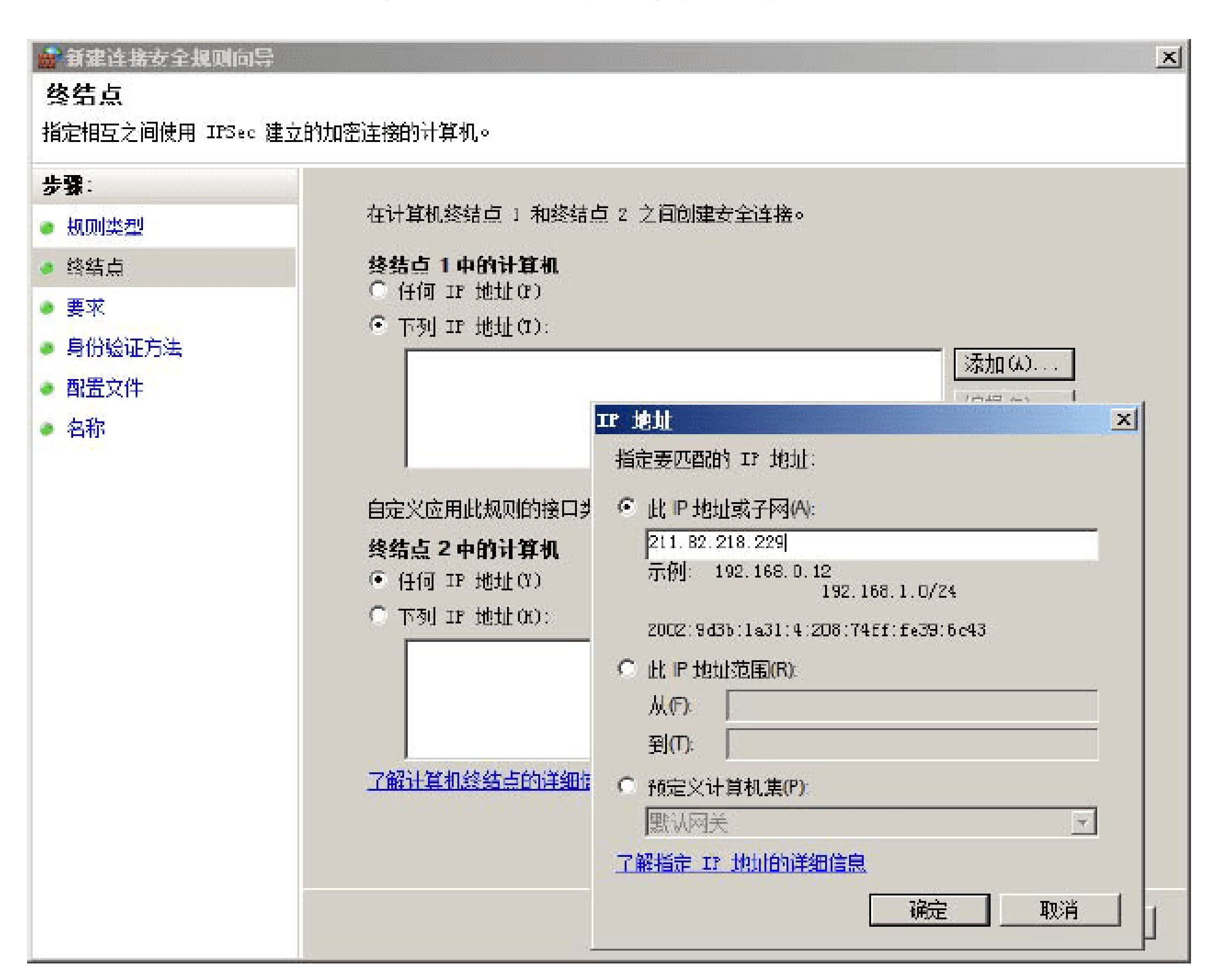


图 8-18 “终结点”界面

- 请求对入站和出站连接进行身份验证：使用此选项要求对所有入站和出站流量进行身份验证，但在身份验证失败时允许连接。如果可以进行身份验证，则将对流量进行身份验证。此选项通常用于低安全性环境或计算机必须可以连接的环境，但不能执行高级安全 Windows 防火墙所具备的身份验证。
- 要求对入站连接进行身份验证并请求对出站连接进行身份验证：使用此选项要求对所有入站流量进行身份验证，否则将阻止该流量。可以对出站流量进行身份验证，但身份验证失败时仍然允许

其通过。如果对出站流量可以进行身份验证，则将对该流量进行身份验证。

- 要求对入站和出站连接进行身份验证：使用此选项要求对所有入站和出站流量进行身份验证，否则将阻止该流量。此选项通常用于高安全性的网络环境，其中流量必须受到保护和控制，且必须能进行连接的计算机可以执行具有高级安全性的 Windows 防火墙所具备的身份验证类型。
- 不进行身份验证：对所有入站和出站连接请求均不进行任何身份验证，此种方式安全性最低。

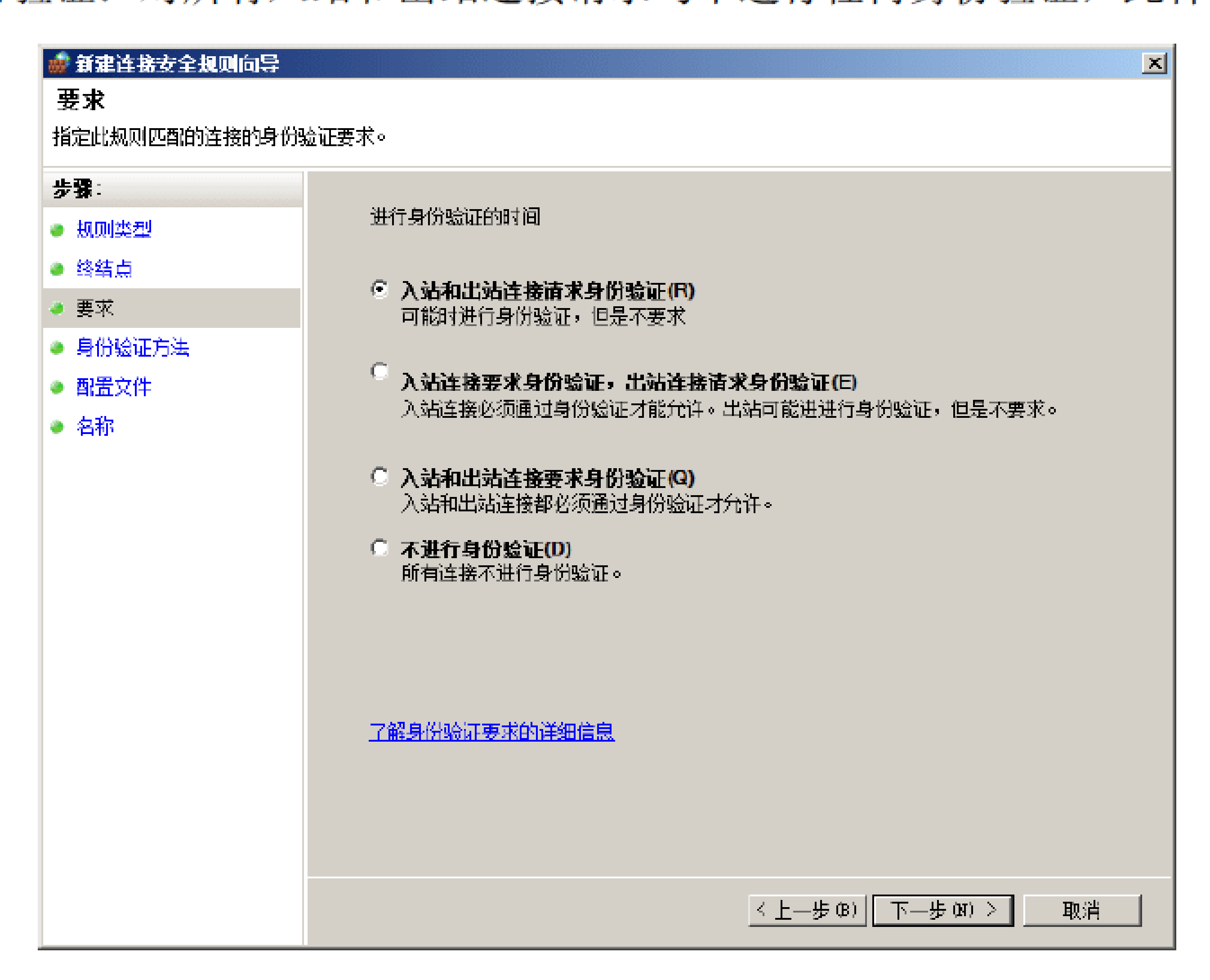


图 8-19　“要求”界面

④　单击“下一步”按钮，显示如图 8-20 所示的“身份验证方法”界面，选择希望使用的身份验证方法，本例选择“默认值”单选按钮。除此之外，用户也可以选择“高级”单选按钮，重新定义自己需要的身份验证方法。



图 8-20　“身份验证方法”界面

⑤　单击“下一步”按钮，显示如图 8-21 所示的“配置文件”界面，选择需要应用规则的配置文件，

系统默认为全部选择。



图 8-21 “配置文件”界面

⑥ 单击“下一步”按钮，显示如图 8-22 所示的“名称”界面，在“名称”和“描述”文本框中，分别输入规则名称和描述即可。

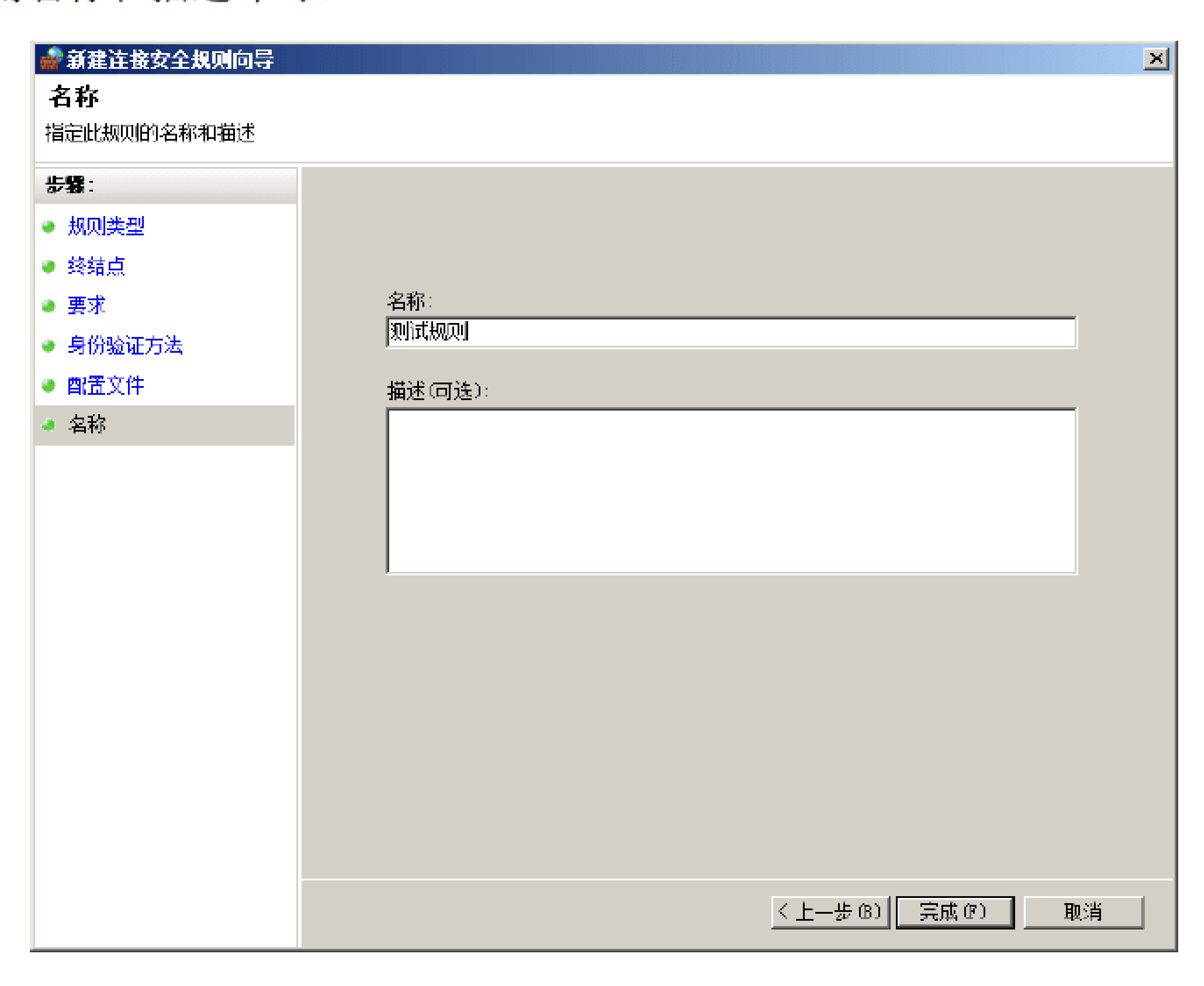


图 8-22 “名称”界面

⑦ 单击“完成”按钮关闭向导，完成新规则的创建。

6. 配置 ICMP 免除

管理员经常使用 ICMP 协议中的 ping 命令来判断服务器是否在线。如果服务器的 IPSec 阻止了管理员的 ping 命令，那么将使管理员误认为服务器不在线。和 IPSec 免除类似，为 ICMP 创建免除也会有轻微的

风险。攻击者可能会使用 ICMP 为网络创建一个地图，从而发动恶意攻击。

① 在高级安全 Windows 防火墙控制台中，右击“本地计算机上的高级安全 Windows 防火墙”，在弹出的快捷菜单中选择“属性”选项，打开如图 8-23 所示的“高级安全 Windows 防火墙-本地组策略对象 属性”对话框，默认为“域配置文件”选项卡。

② 切换到如图 8-24 所示的“IPSec 设置”选项卡，在“从 IPSec 免除 ICMP”下拉列表框中选择“是”选项，单击“确定”按钮即可。



图 8-23　“高级安全 Windows 防火墙-本地组策略对象 属性”对话框



图 8-24　“IPSec 设置”选项卡

8.3　使用组策略配置 Windows 防火墙

从 Windows XP 操作系统(Windows XP HomeEdition 除外)开始，系统就已经集成 Windows 防火墙。因此，在中小型网络环境中，通过使用 Active Directory 和组策略，可以集中配置 Windows 防火墙的设置，并将这些设置应用到所有 Windows XP SP2 客户端计算机。用户可以在 Windows Vista 和 Windows Server 2008 计算机的组策略控制台中，通过如下两种方式配置和管理高级安全 Windows 防火墙。

- “计算机配置”→“Windows 设置”→“安全设置”→“高级安全 Windows 防火墙”→“高级安全 Windows 防火墙-本地组策略对象”：这种节点设置主要应用于 Windows Vista 和 Windows Server 2008。建议用户使用这种方式，因为这里可以提供更加详细的防火墙规则配置，并且允许用户配置新的认证类型和新的加密选项。
- “计算机配置”→“管理面板”→“网络”→“网络连接”→“Windows 防火墙”：这种节点设置主要应用于 Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008。这种方法要比上面那种缺少灵活性；但是，可以应用于所有版本的 Windows 防火墙。如果在 Windows Vista 中使用的不是最新的 IPSec 功能，可以使用这种方式配置所有客户端。

8.3.1　创建组策略

为了达到最好的效果，需要为 Windows XP/Windows Server 2003/Windows Vista/Windows Server

2008 创建单独的组策略，然后使用 WMI 请求定位组策略到运行适当 Windows 版本的计算机。

① 以具有域管理员权限的用户登录到域控制器，单击“开始”→“管理工具”→“组策略管理”命令，打开“组策略管理”窗口。依次展开“林”→“域”→“coolpen.net”选项，右击新建策略应用到的组织单位，选择快捷菜单中的“在这个域中创建 GPO 并在此处链接”命令，显示如图 8-25 所示的“新建 GPO”对话框，在“名称”文本框中，输入希望使用的策略名称，如 Windows 防火墙。

② 单击“确定”按钮，返回如图 8-26 所示的“组策略管理”窗口。

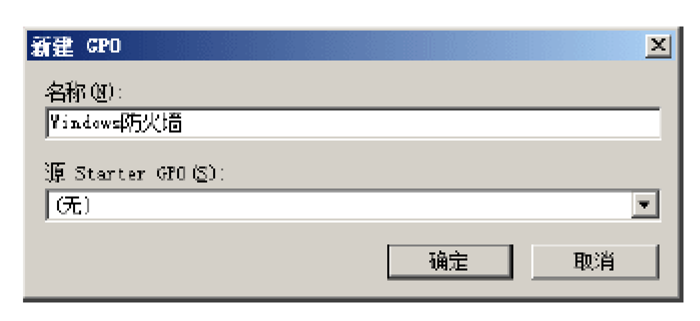


图 8-25 “新建 GPO”对话框

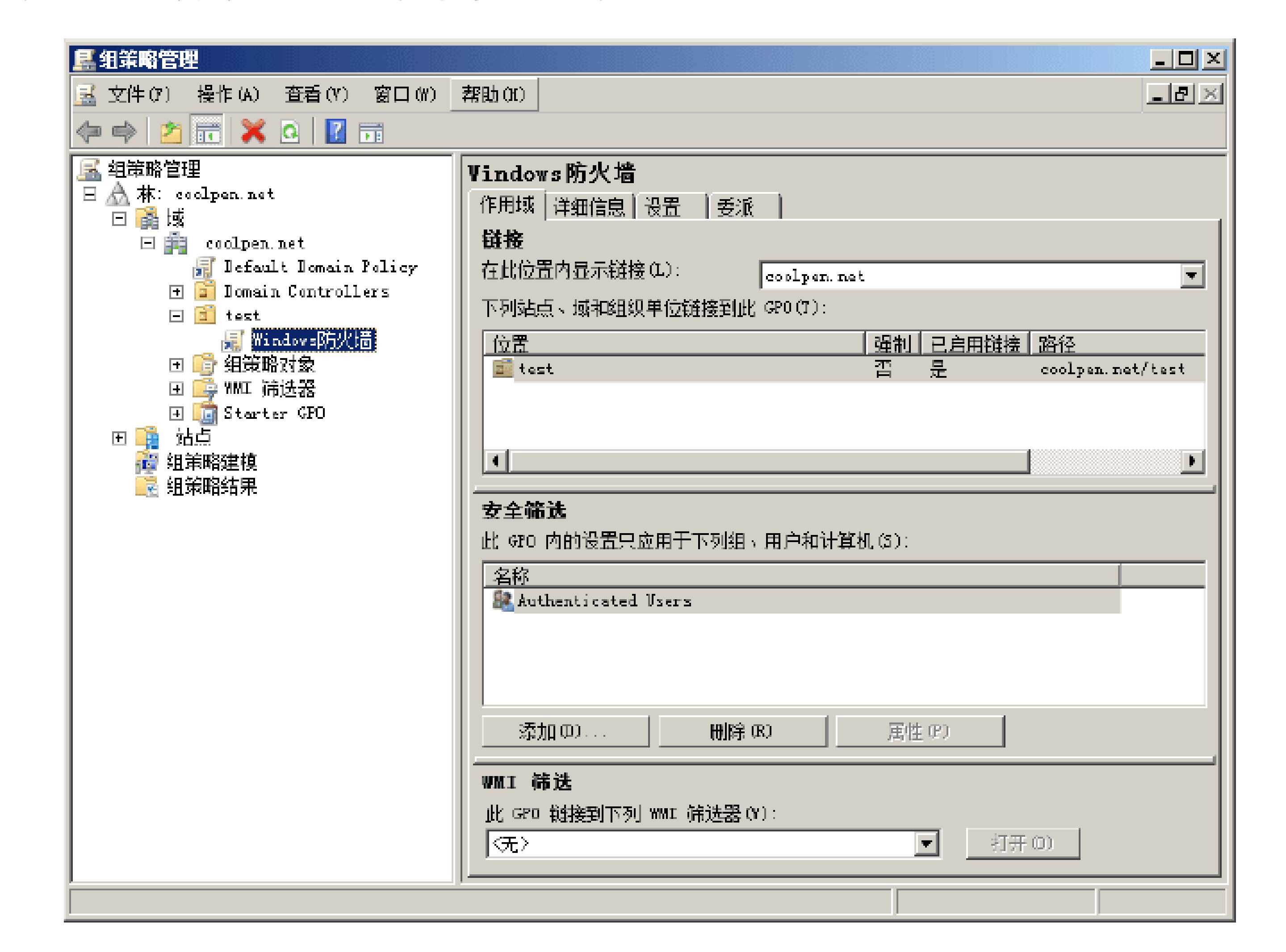


图 8-26 “组策略管理”窗口

③ 右击“Windows 防火墙”，选择快捷菜单中的“编辑”命令，显示如图 8-27 所示的“组策略管理编辑器”窗口，依次展开“计算机配置”→“策略”→“管理模板”→“网络”→“网络连接”→“Windows 防火墙”选项。

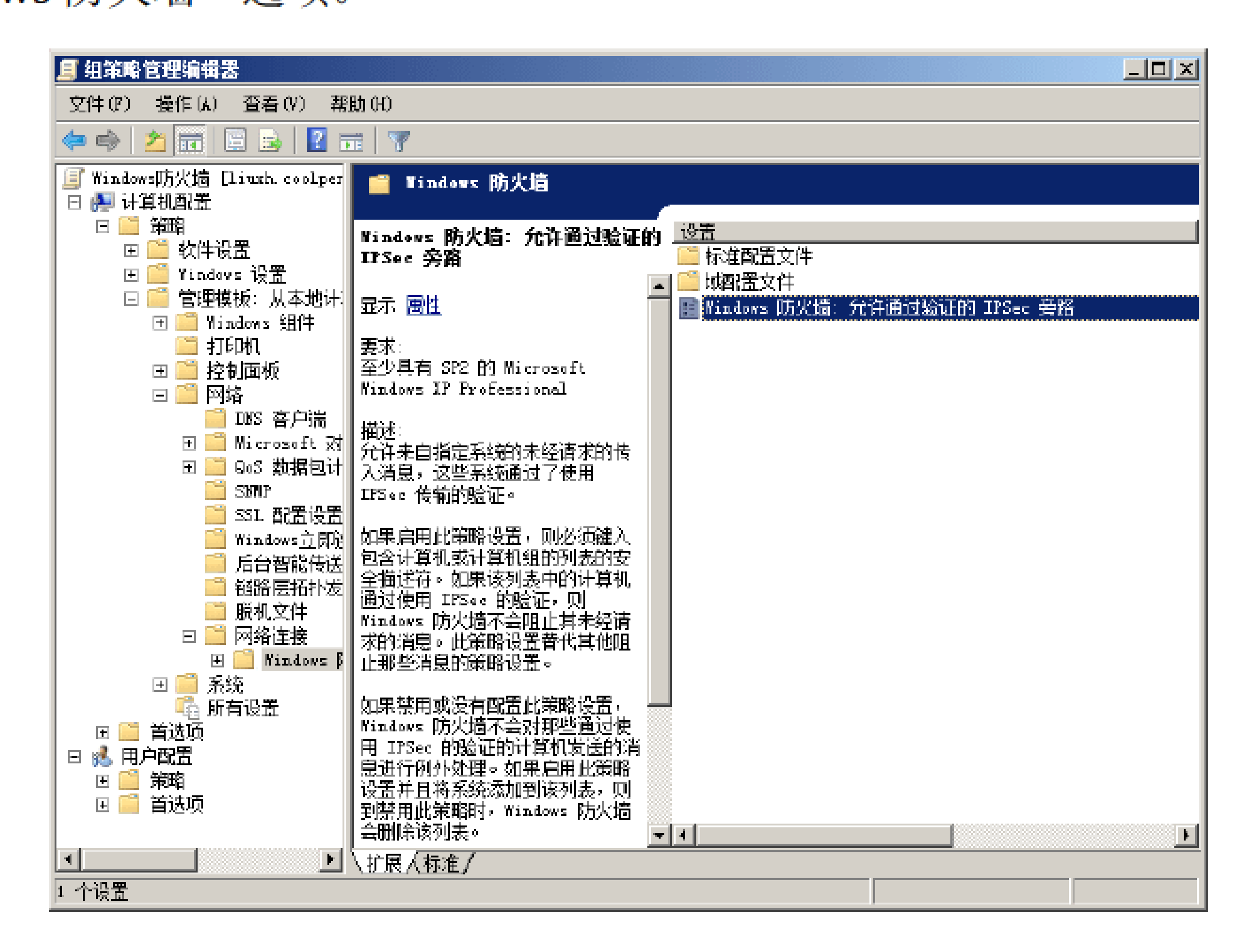


图 8-27 “组策略管理编辑器”窗口

8.3.2　Windows 防火墙：允许通过验证的 IPSec 旁路

该策略将允许来自指定系统的未经请求的传入消息，如果启用该策略设置，必须输入包含计算机或计算机组的列表的安全描述符。如果列表上的计算机通过使用 IPSec 的验证，Windows 防火墙不会阻止未经请求的消息。如果禁用或不配置该策略设置，Windows 防火墙不会对计算机发送的消息进行例外处理，即使计算机通过了 IPSec 的验证。

在“组策略管理编辑器”窗口中，双击“Windows 防火墙：允许通过验证的 IPSec 旁路”策略，打开如图 8-28 所示的“Windows 防火墙：允许通过验证的 IPSec 旁路 属性”对话框。根据需要选择“已启用”或者“已禁用”单选按钮，即可完成策略的设置。

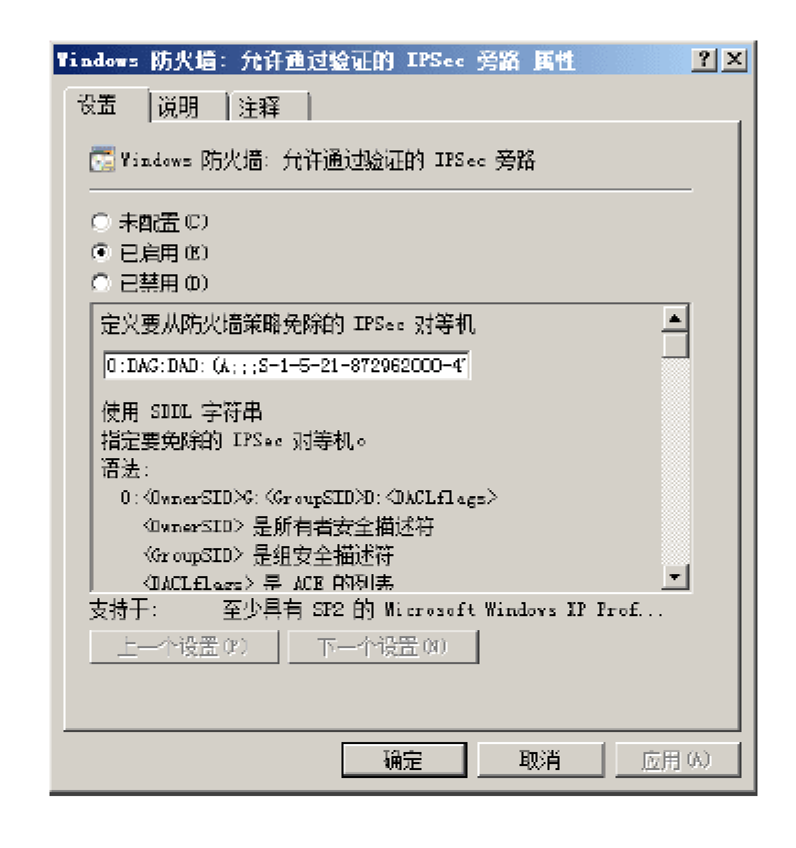


图 8-28　“Windows 防火墙：允许通过验证的 IPSec 旁路 属性”对话框

8.3.3　标准配置文件/域配置文件

Windows 防火墙配置文件分为标准配置文件和域配置文件。标准配置文件是基于本地计算机的 Windows 防火墙配置；域配置文件是基于 AD 的网络防火墙配置。标准配置文件和域配置文件下的子策略所完成的功能，与“Windows 防火墙”设置所完成的功能相同。

这里以域配置文件为例，介绍如何在组策略下配置 Windows 防火墙。打开组策略控制台，依次展开“计算机配置”→“Windows 设置”→“管理模板”→“网络”→“网络连接”→“Windows 防火墙”→“域配置文件”选项，在右侧列表中显示 Windows 防火墙域配置文件策略中的所有子策略，如图 8-29 所示。

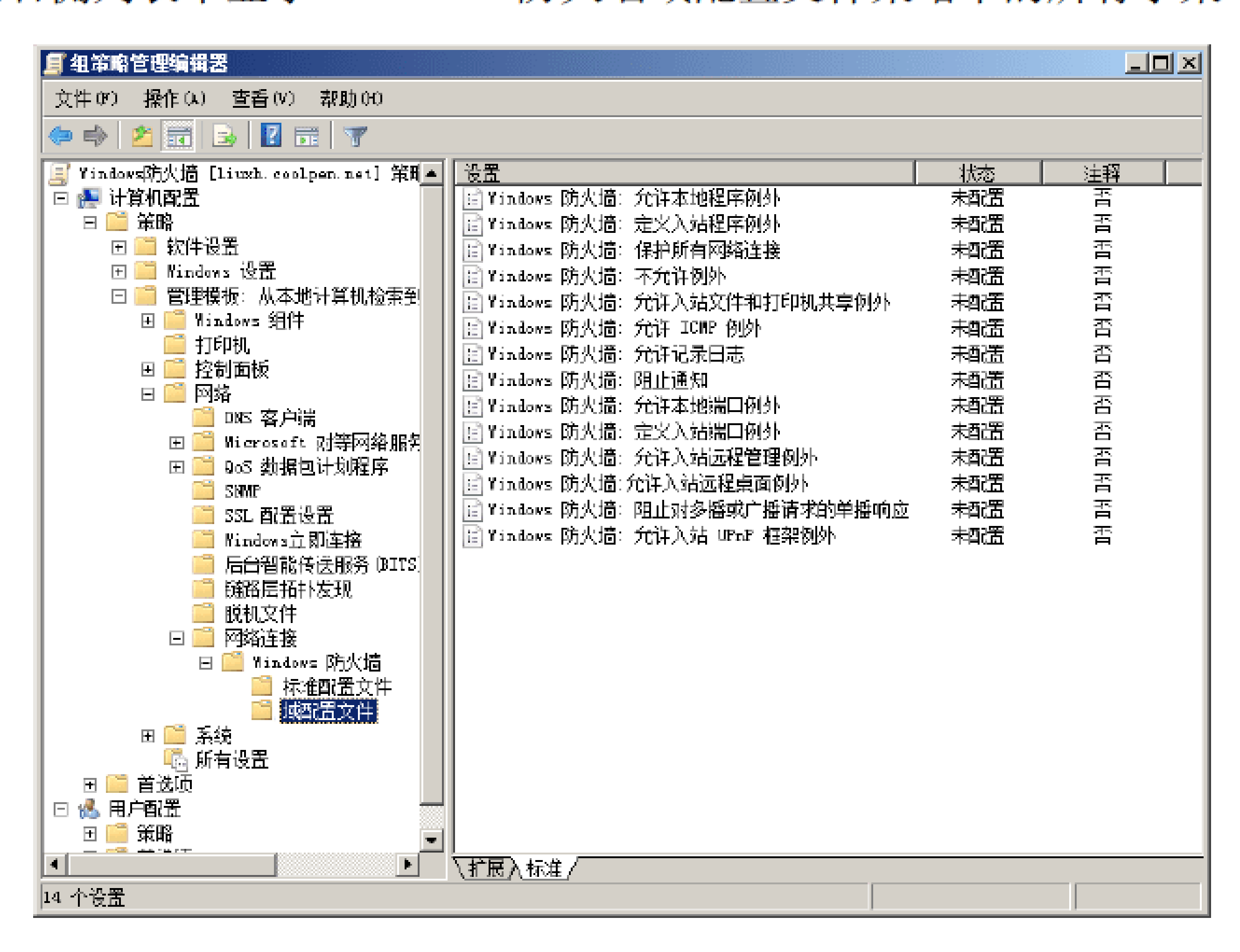
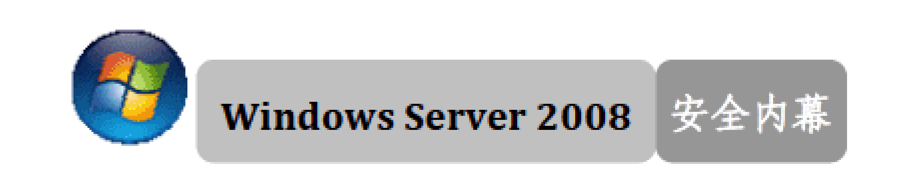


图 8-29　域配置文件窗口

例如，配置“Windows 防火墙：允许本地程序例外”策略。如果启用该策略设置，将允许用户在 Windows 防火墙组件中向本地程序中添加例外列表。双击右侧窗口中的“Windows 防火墙：允许本地程序例外”策



略，打开“Windows 防火墙：允许本地程序例外 属性”对话框，如图 8-30 所示。根据需要选择“已启用”单选按钮，即可启用该策略。

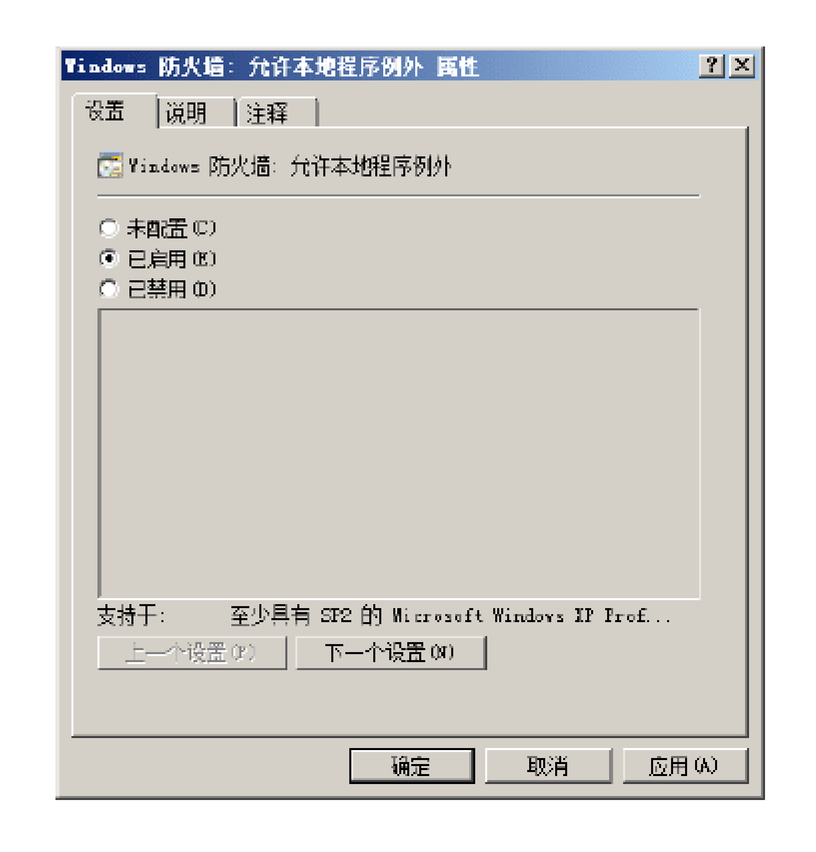


图 8-30　“Windows 防火墙：允许本地程序例外 属性”对话框

8.4　配置 Windows 防火墙事件审核

默认情况下，系统没有启用对 Windows 防火墙的事件审核设置。如果需要确定应用过程中，哪些应用程序或端口被设置为例外，或者处理运行故障时，启用 Windows 防火墙日志、Windows 防火墙审核和网络跟踪会很有帮助。管理员可以通过查看时间查看器中的相关日志，详细了解工作过程中的状态变化。

8.4.1　启用审核设置

若要配置 Windows 防火墙事件审核，必须以具有系统管理员权限的用户账户登录系统，启用本地策略中的“审核策略更改”、“审核进程跟踪”和“审核系统事件”策略。单击“开始”按钮，在“开始搜索”文本框中输入 gpedit.msc，按 Enter 键显示如图 8-31 所示的“本地组策略编辑器”窗口。如果是在域环境中部署所有客户端 Windows 防火墙，则直接以域管理员账户编辑域策略中的相关设置即可。

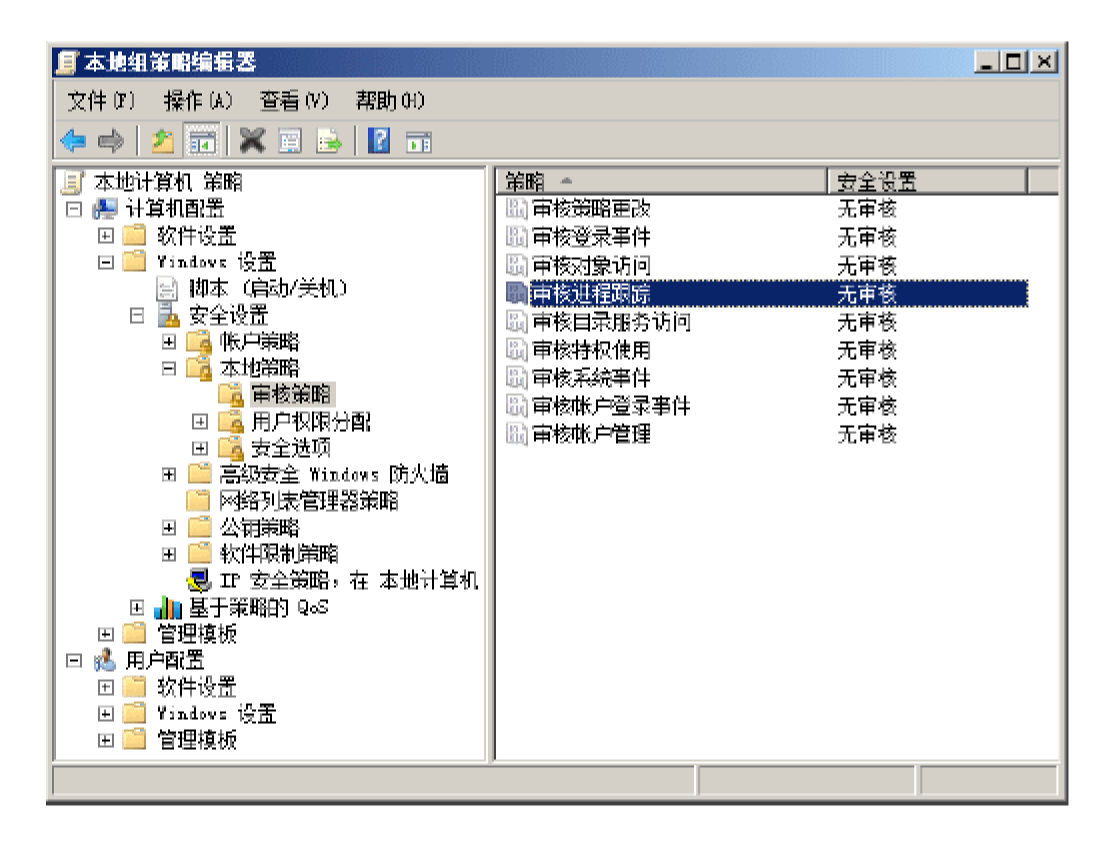


图 8-31　“本地组策略编辑器”窗口

1. 审核策略更改

在“本地组策略编辑器”窗口中，双击“审核策略更改”策略，显示如图 8-32 所示的“审核策略更改属性”对话框。选中“成功”或者“失败”复选框，单击“确定”按钮，即可完成策略的设置。

审核策略更改产生的安全事件中，与 Windows 防火墙相关的事件如表 8-2 所示。

表 8-2 与 Windows 防火墙相关的策略更改事件

事件 ID	消 息
4944	Windows 防火墙启动时下列策略处于活动
4945	Windows 防火墙启动时被列出规则
4946	Windows 防火墙例外列表已被进行更改，添加规则
4947	Windows 防火墙例外列表已被进行更改，修改规则
4948	Windows 防火墙例外列表已被进行更改，删除规则
4949	Windows 防火墙设置已还原为默认值
4950	Windows 防火墙设置已经更改
4951	规则已忽略，因为通过 Windows 防火墙无法识别其主版本号
4952	由于通过 Windows 防火墙无法识别其次要版本号部分规则已被忽略，将强制规则的其他部分
4953	因为无法解析规则，已忽略通过 Windows 防火墙
4954	Windows 防火墙组策略设置已更改，已应用新设置
4956	Windows 防火墙已更改活动配置文件
4957	Windows 防火墙未应用以下规则
4958	由于规则引用此计算机上没有配置项目，没有 Windows 防火墙采用以下规则

2. 审核进程跟踪

在“本地组策略编辑器”窗口中，双击“审核过程跟踪”策略，显示如图 8-33 所示的“审核进程跟踪属性”对话框。根据需要选中“成功”或者“失败”复选框，单击“确定”按钮，即可完成策略的设置。

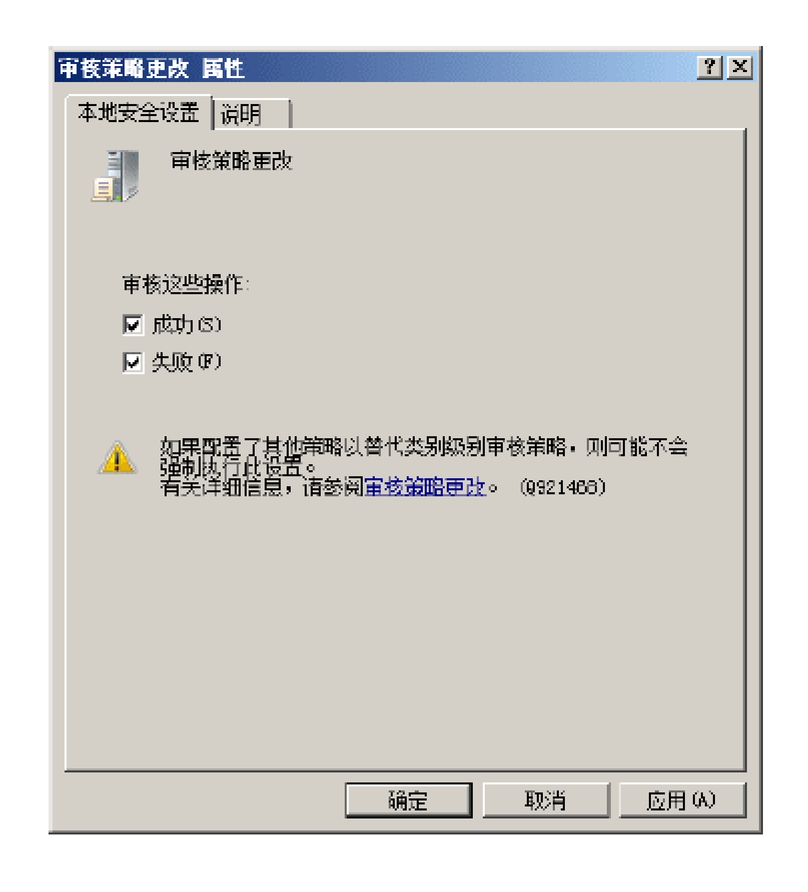



图 8-32 “审核策略更改 属性”对话框

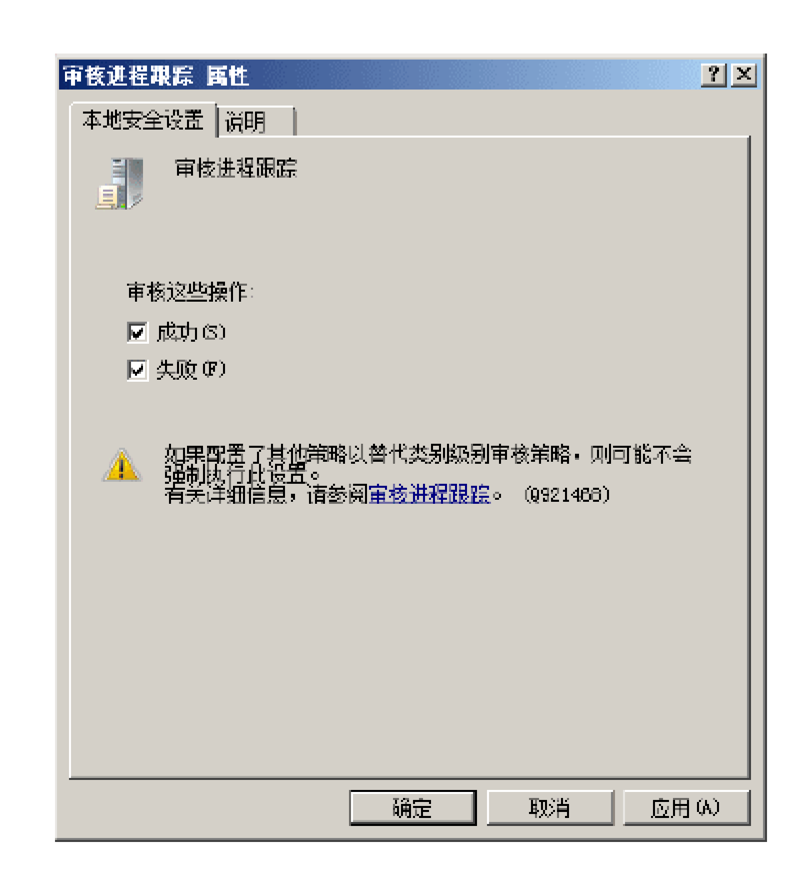


图 8-33 “审核进程跟踪 属性”对话框

由“审核详细跟踪”安全策略设置所生成的安全事件如表 8-3 所示。

表 8-3 审核进程跟踪事件

事件 ID	消 息
4688	已创建一个新进程
4689	进程已退出
4692	尝试数据保护主密钥备份
4693	尝试对数据保护主密钥进行恢复
4694	尝试保护的审计保护数据
4695	尝试未保护的审计保护数据
4696	主令牌被分配给处理
5712	试图远程过程调用(RPC)

3. 审核系统事件

审核系统事件中包括 Windows 防火墙应用程序的工作过程，如启动、停止等。在“本地组策略编辑器”窗口中，双击“审核系统事件”策略，显示如图 8-34 所示的“审核系统事件 属性”对话框。根据需要选中“成功”或者“失败”复选框，单击“确定”按钮，即可完成策略的设置。

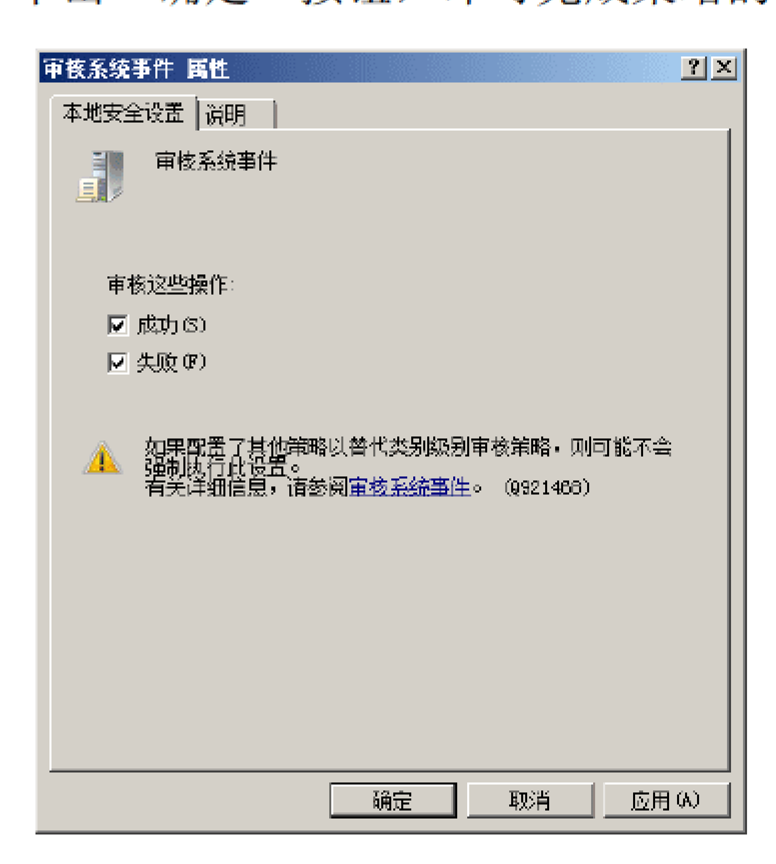


图 8-34 “审核系统事件 属性”对话框

审核策略更改产生的安全事件中，与 Windows 防火墙相关的事件如表 8-4 所示。

表 8-4 与 Windows 防火墙相关的系统事件

事件 ID	消 息
5024	Windows 防火墙服务成功启动
5025	Windows 防火墙服务已停止
5027	Windows 防火墙服务无法从本地存储器检索安全策略。服务将继续强制当前策略
5028	Windows 防火墙服务无法分析新安全策略。服务将继续强制当前实施策略
5029	Windows 防火墙服务无法初始化驱动程序。服务将继续强制当前策略
5030	Windows 防火墙服务无法启动
5032	Windows 防火墙无法通知用户阻止应用程序接受传入连接在网络上

续表

事件 ID	消 息
5033	Windows 防火墙驱动程序成功启动
5034	Windows 防火墙驱动程序已停止
5035	Windows 防火墙驱动程序无法启动
5037	Windows 防火墙驱动程序检测到关键运行错误，终止

8.4.2 查看 Windows 防火墙事件

启用审核策略后，即可通过 Windows Server 2008 系统的事件查看器，查看和管理 Windows 防火墙工作过程中产生的安全事件。事件日志中记录了事件发生的时间、事件来源、用户账户、操作代码及了解详细相关信息的超级链接。在 Windows Server 2008 系统中，事件日志详细信息的基础结构完全符合 XML 架构，而且可以访问代表指定事件的 XML。这也是 Windows Server 2008 区别于 Windows Server 2003 的主要方面之一。

① 单击“开始”→“管理工具”→“事件查看器”命令，打开“事件查看器”窗口，依次展开“Windows 日志”→“安全”选项，如图 8-35 所示。系统默认已经启动“预览窗格”功能，即在事件列表中选择时间后，将自动显示相应预览信息。

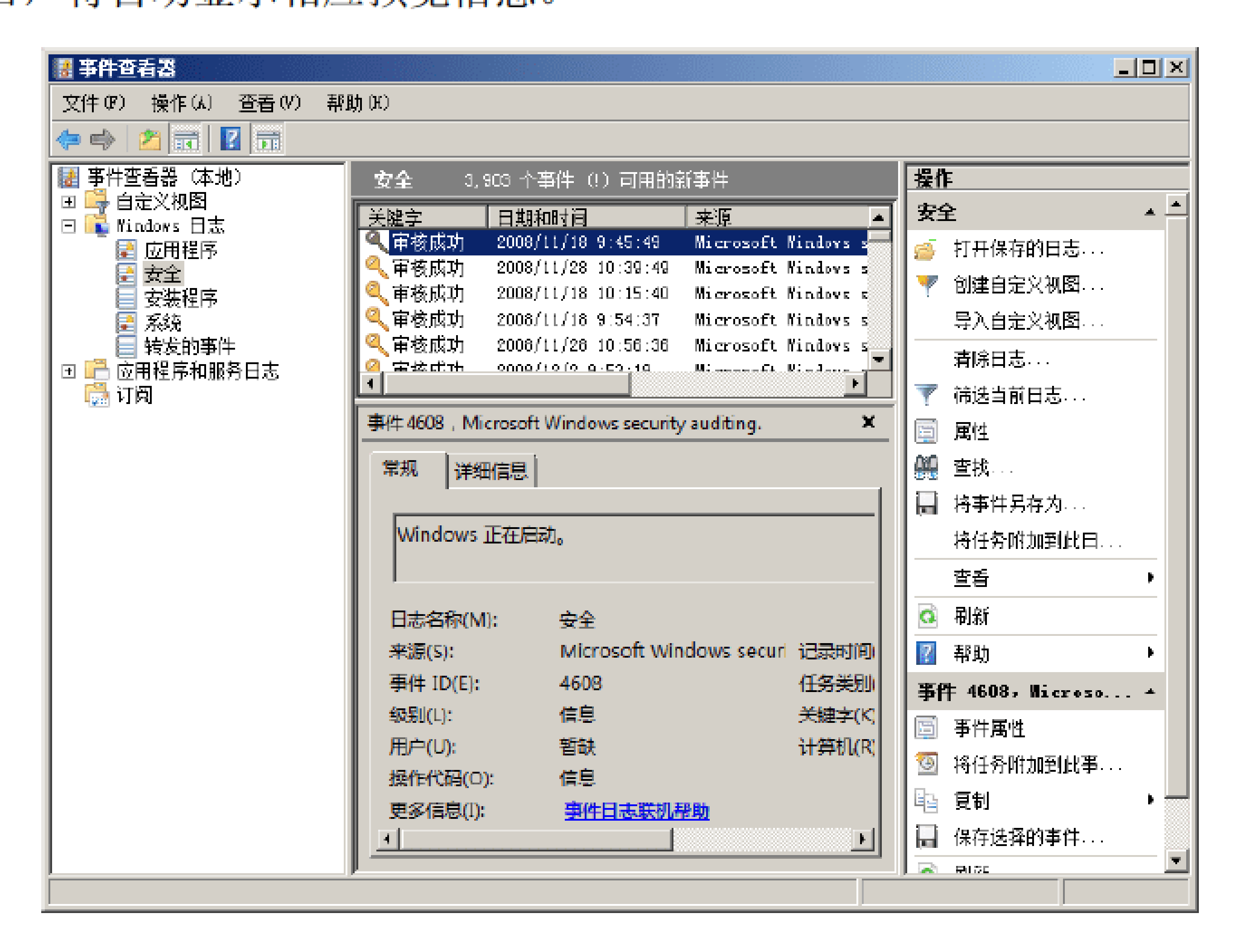


图 8-35 “事件查看器”窗口

② 单击“事件 ID”标签，按照时间 ID 排序后，找到希望查看的 Windows 防火墙事件即可。双击事件打开如图 8-36 所示的“事件属性 – 事件 5024”对话框，在“常规”选项卡中，可以查看该事件的来源、类型、级别、时间等信息。

③ 单击“详细信息”标签，切换至如图 8-37 所示的“详细信息”选项卡，系统默认以“友好视图”方式显示。

④ 选择“XML 视图”单选按钮，即可以 XML 视图方式显示事件详细信息，如图 8-38 所示。

⑤ 单击“关闭”按钮，关闭“事件属性”对话框即可。

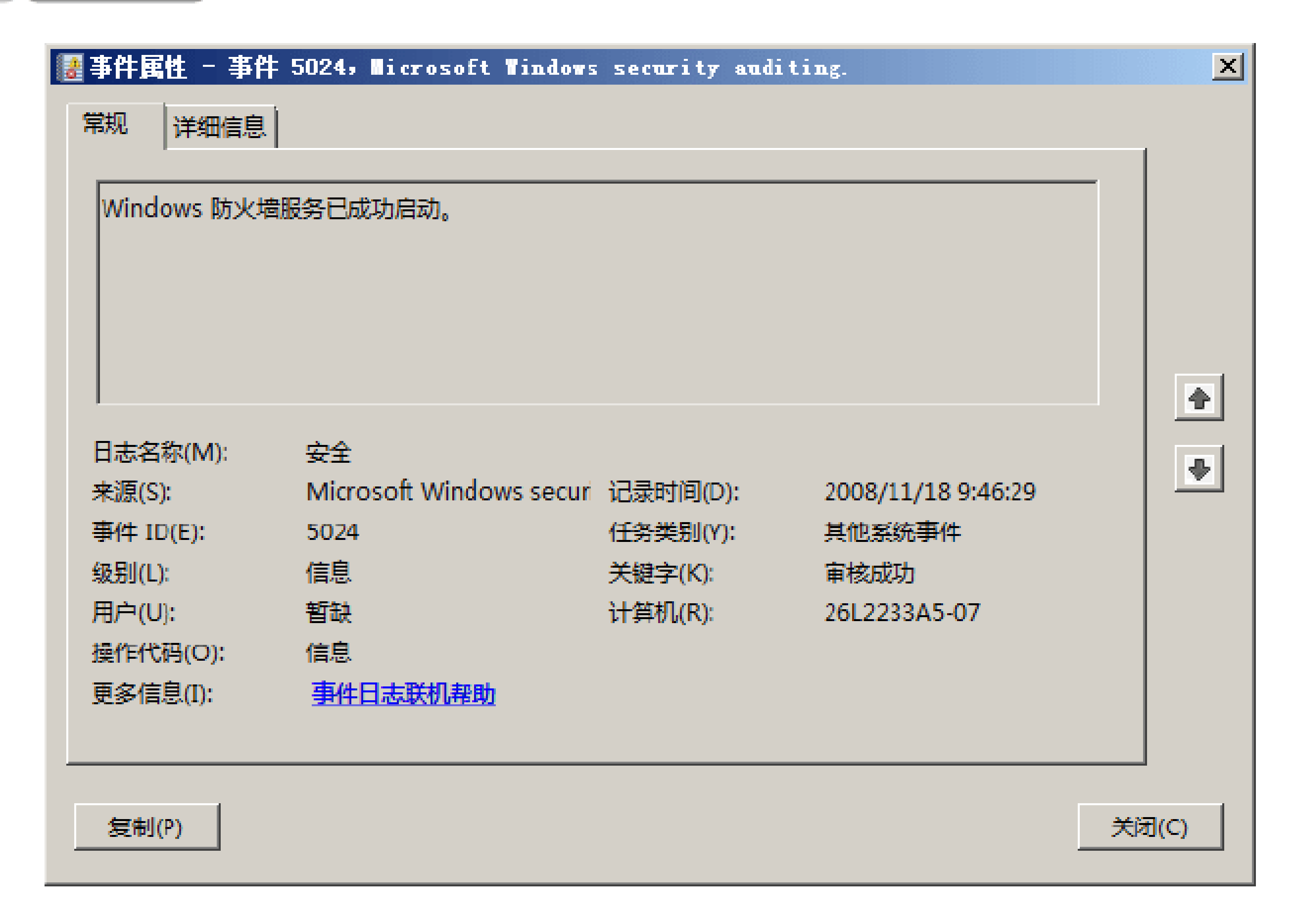


图 8-36 “事件属性 – 事件 5024”对话框

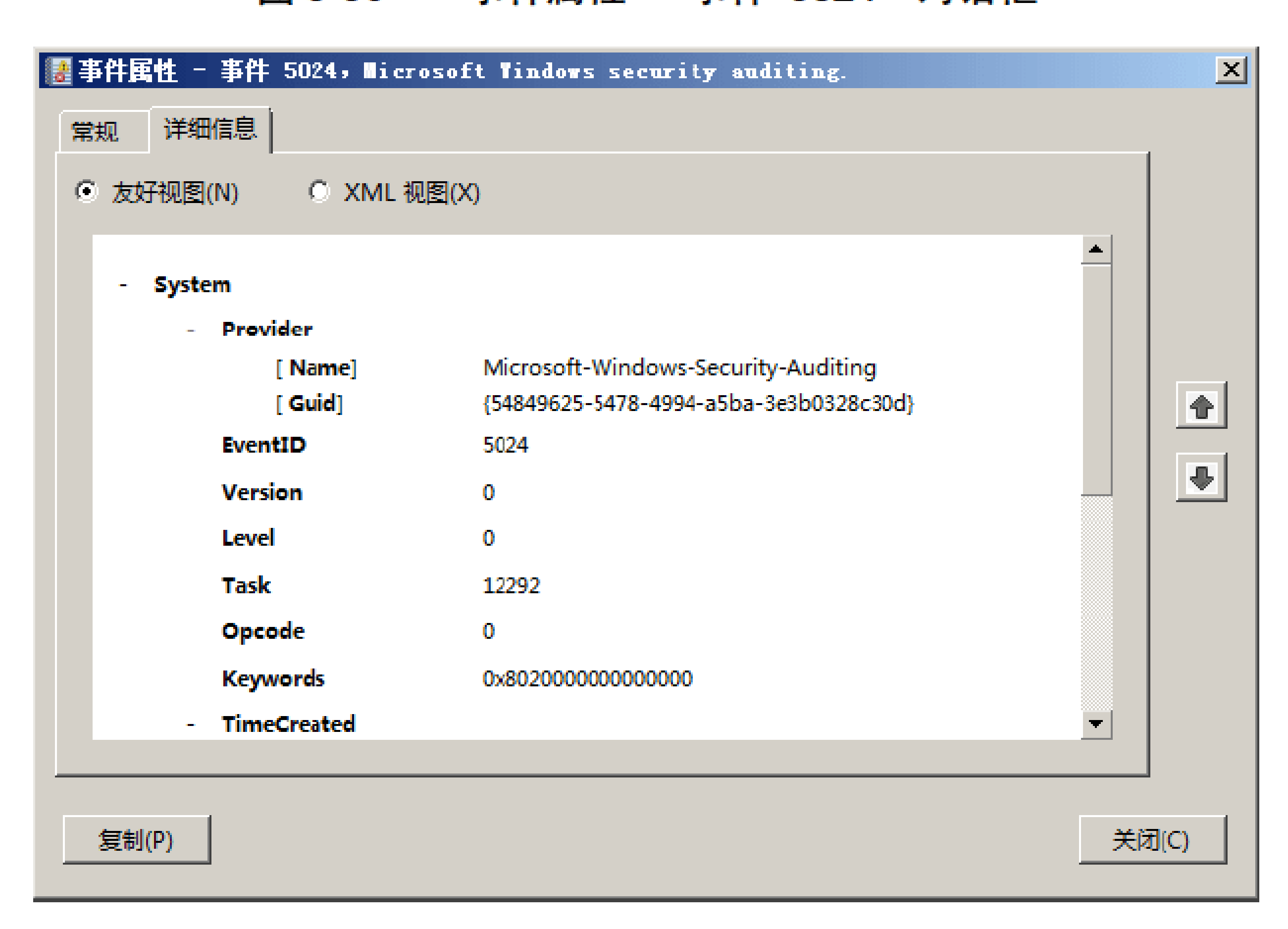


图 8-37 “详细信息”选项卡

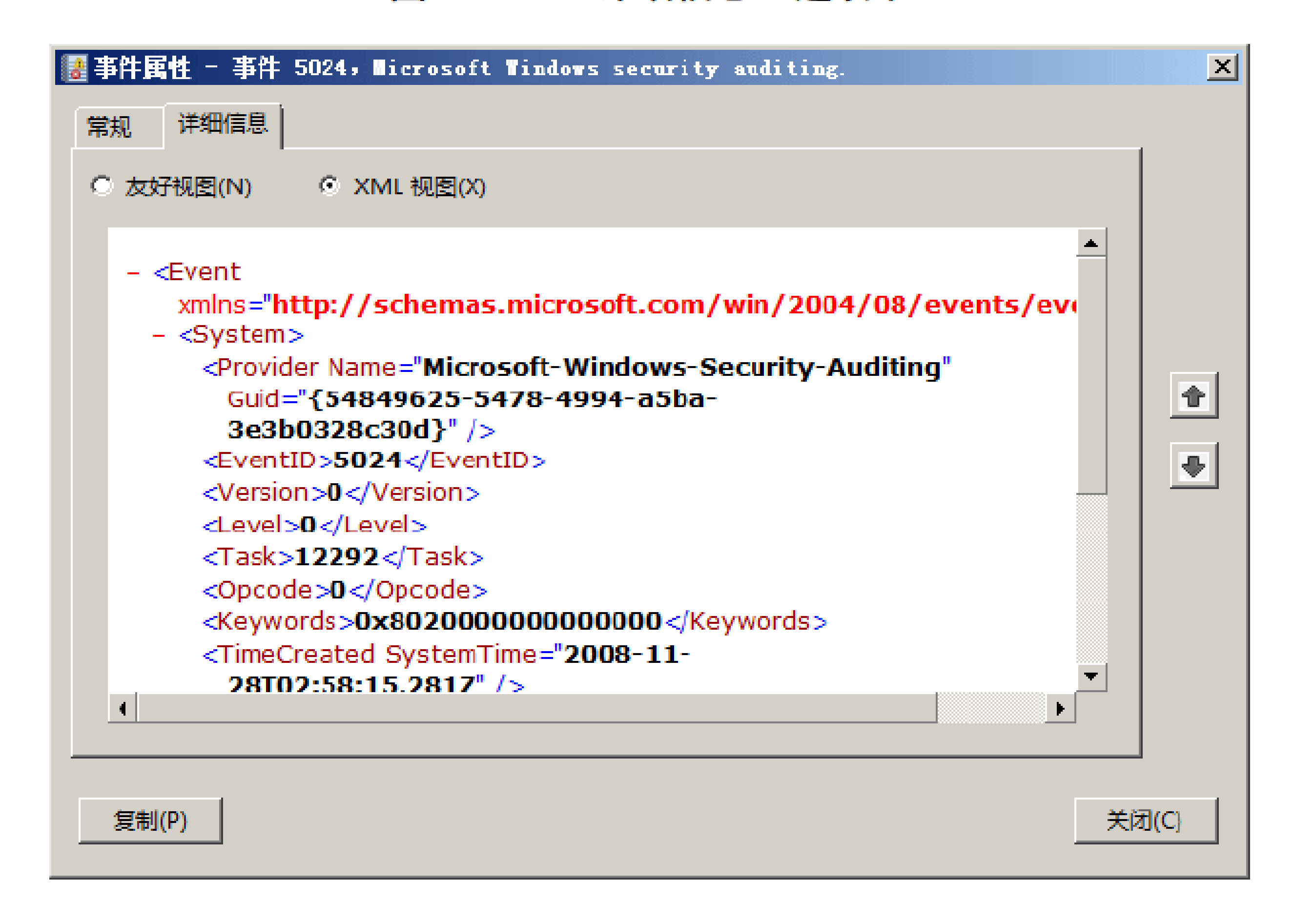


图 8-38 XML 视图

8.4.3 筛选 Windows 防火墙事件

启动任何一项审核策略都会产生大量的事件日志，而其中与 Windows 防火墙运行相关的内容并不多。通过筛选相关日志，可以快速查看需要的目标事件。在事件筛选器中，用户可以指定关键字、事件 ID、事件来源等筛选信息。

① 在“事件查看器”窗口中，依次展开“Windows 日志”→“安全”选项。在“操作”栏中单击“筛选当前日志”链接，打开如图 8-39 所示的“筛选当前日志”对话框。例如按照事件 ID 筛选，在“包括/排除事件 ID”文本框中，输入希望查看的事件 ID 号或 ID 范围。



提示： 如果要查看多个事件，则 ID 号之间必须以逗号分隔。如果要包括一个范围的 ID，例如 5024 到 5033(包括 5033)，则可以输入“5024-5033”。如果希望筛选器显示包括除某些 ID 以外所有 ID 的事件，则输入这些排除的 ID，前面加一个减号。例如，若要包括 5024 和 5033 之间除 5032 以外的所有 ID，则可以输入“5024-5033,-5032”。

② 单击“确定”按钮，即可开始筛选。完成后，显示如图 8-40 所示的结果。直接在“已筛选日志”列表中，双击希望查看的事件日志即可。

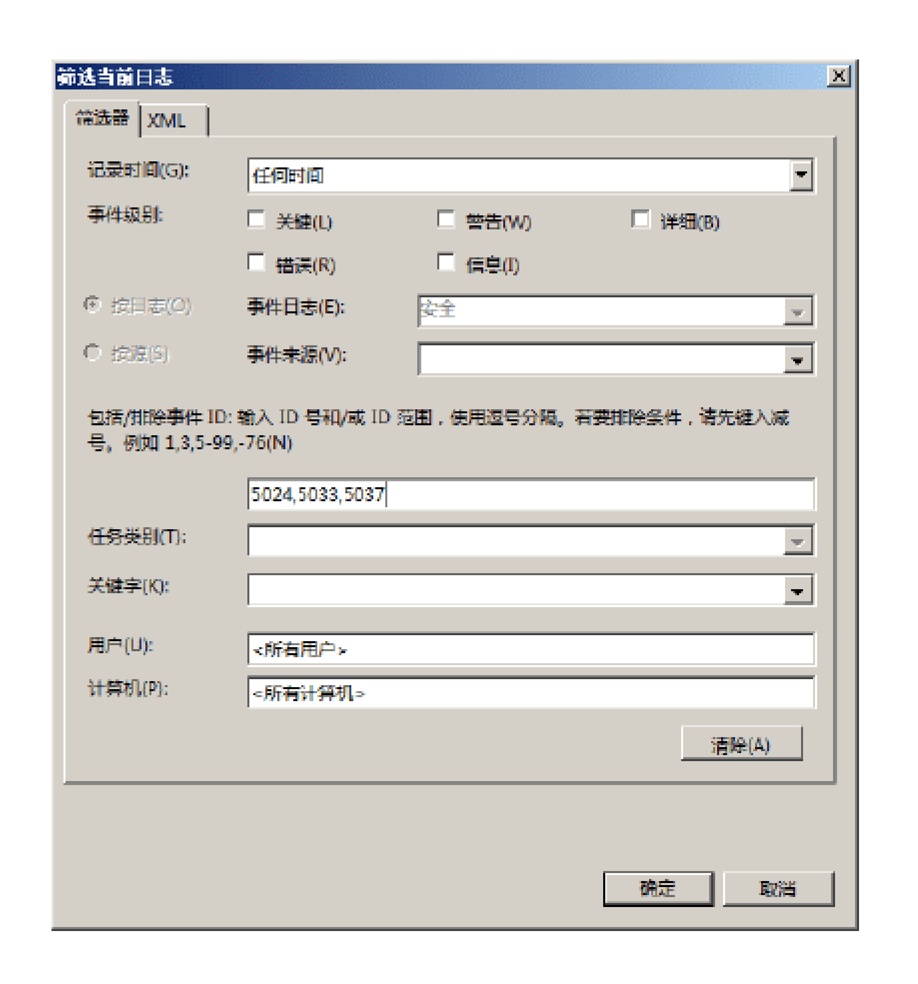


图 8-39 “筛选当前日志”对话框

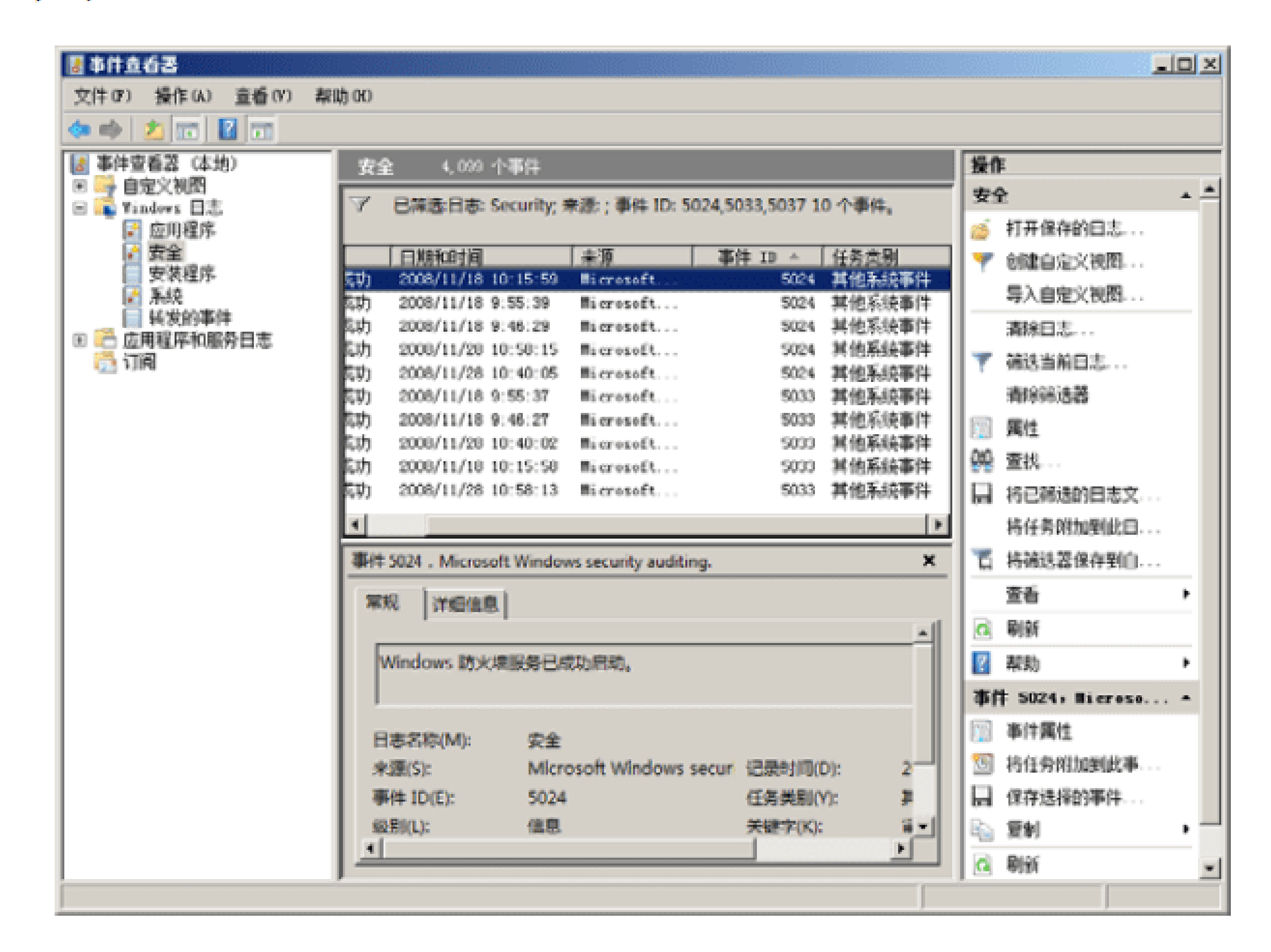


图 8-40 筛选事件日志

③ 单击“清除筛选器”链接，即可清除当前筛选结果，返回相应的事件分组。

8.4.4 配置 Windows 防火墙日志文件

Windows 防火墙应用程序本身在运行过程中，也会产生相应的日志。与系统事件不同的是，这些日志主要记录运行过程中各个防火墙规则的变化情况，并且用户可以为不同作用域的防火墙规则指定不同的日志文件。需要注意的是，该日志默认是未配置的，即不对任何规则执行情况进行记录。

① 打开“高级安全 Windows 防火墙”窗口，右击“本地计算机 上的高级安全 Windows 防火墙”，在弹出的快捷菜单中选择“属性”命令，打开如图 8-41 所示的“本地计算机 上的高级安全 Windows 防火墙 属性”对话框。

② 在“日志”选项区中单击“自定义”按钮，显示如图 8-42 所示的“自定义 专用配置文件 的日志设置”对话框。在“名称”文本框中，显示的是日志文件的默认保存路径和名称：%Systemroot%\System32\LogFiles\Firewall\pfirewall.log。在“大小限制”文本框中，可以自定义日志文件的最大值，以确保不丢失任何信息。在“记录被丢弃的数据包”和“记录成功的连接”下拉列表框中，均选择“是”选项即可；系统默认选择“否”选项，即不启用日志。



图 8-41 “本地计算机 上的高级安全 Windows 防火墙 属性”对话框

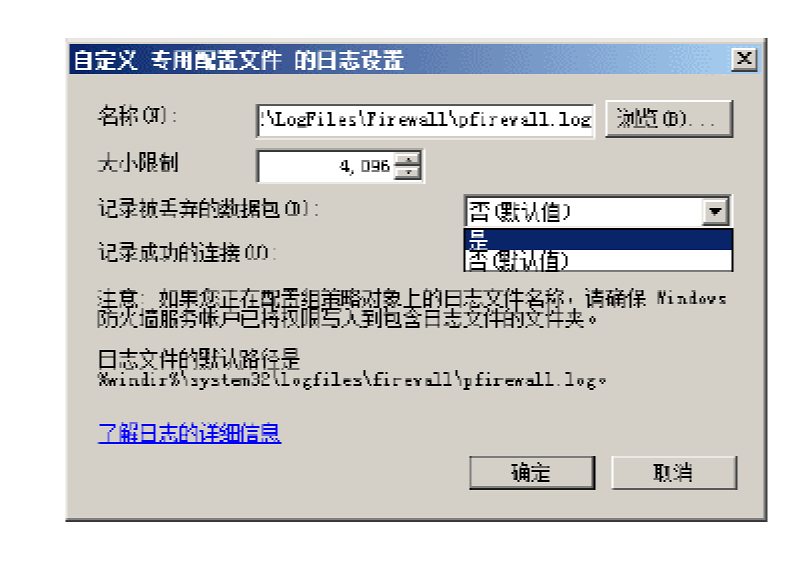


图 8-42 “自定义 专用配置文件 的日志设置”对话框

③ 单击“确定”按钮，保存设置即可。

在“专用配置文件”和“公用配置文件”选项卡中，同样可以对相应作用域的防火墙规则配置日志文件。既可以使用和“域配置文件”相同的目标日志文件，也可以重新指定。为了便于查看和管理，建议为不同作用范围的防火墙规则指定不同的日志文件。

8.5 Windows 防火墙的维护

Windows 防火墙的运行维护主要包括以下内容。

- 当新的服务器应用程序安装后，为其调整入站筛选规则。
- 对于不支持 IPSec 的计算机和网络添加连接安全规则的免除功能。
- 当 IP 地址变化时升级规则，可以通过修改高级安全 Windows 防火墙控制台中的规则属性完成。
- 当计算机升级操作系统时，移除免除(或者扩展现有规则覆盖范围)。

因为 Windows 防火墙的变动有着严重的安全牵连，所有的变动都要按照微软操作构架(MOF)来进行，大致过程如下。

- 请求改变：提交一份请求变化的文档后才能正式开始改变。
- 分类改变：为改变分配一个优先级和类别，根据在基础设备和用户中的紧急程度和影响来进行改变。这种分配将影响执行速度和路由。
- 认证改变：这种改变与否取决于应用程序功能性、网络性能和安全威胁。
- 发展改变：计划这项改变，包括在实验环境中进行测试，决定新的规则是否可以配置到试点组的所有计算机上。
- 释放改变：在生产环境中释放和更改这项设置。
- 重现改变：执行后回顾这项改变是否达到了目的，然后决定是保持这项改变还是回复到原来的状态。

第 9 章　事件和日志

一旦发生系统入侵事件，安全管理员首先要清楚攻击类型、事件和目标应用程序，以便采取相应的补救措施。系统事件日志就是这一切重要信息的唯一来源。根据 Windows Server 2008 系统的事件日志功能，通过“事件查看器”可以查看所有系统日志，以及已安装网络服务的运行日志。通过系统提供的“性能计数器警报”功能，还可以为服务器的相关功能设置警报阀值，如 CPU、内存、进程、文件访问等运行情况，一旦达到阀值，系统将自动向管理员发出警告，做到防患于未然。

关键词

- 事件查看器
- 安全性日志
- 可靠性和性能

9.1 事件查看器

Windows 事件查看器可用于浏览和管理事件日志，是监视系统的运行状况以及在出现问题时解决问题的必不可少的工具。通常情况下，计算机存储的日志类型包括 Windows 系统日志、服务器角色日志、应用程序和服务日志。其中，Windows 系统日志是系统默认的，包括应用程序、安全、安装程序、系统和转发的事件等 5 部分，服务器角色日志和应用程序日志则取决于当前服务器运行服务和应用程序。

9.1.1 事件基本信息

事件日志类似于日记，主要用于记录某一系统事件发生的日期、时间等基本信息，事件是操作系统在某一时刻对某一系统资源或者网络资源发生的访问操作，而记录的一系列行为。该行为包含当前的日期、时间、用户、计算机、来源、事件、类型、分类等信息。表 9-1 中列出了事件的基本要素及描述。

表 9-1 事件基本信息

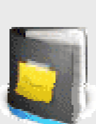
要 素	描 述
日期和时间	事件发生的日期和时间。事件的日期和时间以世界协调时间(UTC)存储，但始终按查看者的区域设置显示
用户	事件发生所代表的用户的名称。如果事件实际上是由服务器进程所引起的，则该名称为客户 ID；如果没有发生模仿的情况，则为主 ID。在可用时，安全日志条目包括主 ID 和模仿 ID。当该服务器允许一个进程采用另一个进程的安全属性时，则产生模仿
计算机	产生事件的计算机的名称。这通常是用户自己的计算机的名称，除非在另一台计算机上查看事件日志
来源	记录事件的应用程序，它可为程序名(如 SQLServer)、系统的组件(如驱动程序)或大程序的组件。例如，Elnkii 指示 EtherLinkII 驱动程序。“来源”始终使用其原始语言
事件 ID	标识此来源的特定事件类型的数字。说明的第一行一般包含事件类型的名称。例如，6005 是在启动事件日志服务时所发生事件的 ID。这类事件说明的第一行是“事件日志服务已启动”。通过结合使用“来源”和“事件”的值，产品支持代理可解决系统问题
级别	事件严重性的分类，包括信息、警告、错误、关键、Success Audit、审核失败等 6 个级别。在“事件查看器”中的正常列表方式下查看，它们都由一个符号表示
操作代码	包含标识活动或应用程序引起事件时正在执行的活动中的点的数字值。例如，初始化或关闭
日志	已记录事件的日志的名称
任务类别	用于表示事件发行者的子组件或活动
关键字	可用于筛选或搜索事件的一组类别或标记，包括“网络”、“安全”或“未找到资源”

9.1.2 事件的类型

Windows 操作系统中定义了 6 种事件类型，系统管理员可以根据关注的事件的性质筛选希望查看的事件。表 9-2 列出了 Windows 系统定义的事件类型，及每个事件类型的具体含义。

表 9-2 事件类型及描述

事件类型	描 述
错误	指明出现了问题，这可能会影响触发事件的应用程序或组件外部的功能。例如，如果在启动过程中某个服务加载失败，将会记录“错误”事件
警告	指明出现的问题可能会影响服务器或导致更严重的问题(如果未采取措施)。例如，当磁盘空间不足时，将会记录“警告”事件
信息	指明应用程序或组件发生了更改，如操作成功完成、已创建了资源，或已启动了服务
关键	指明出现了故障，导致触发事件的应用程序或组件可能无法自动恢复
Success Audit	指明用户权限练习成功
审核失败	指明用户权限练习失败



提示：Success Audit 和“审核失败”类型事件属于严重安全级别，可能出现在安全日志中。

9.1.3 事件查看器的使用

Windows 事件查看器的主要功能就是为管理员提供简洁、快速的时间浏览界面。网络管理员应该养成良好的习惯，经常查看日志，这样可以有效避免突如其来的灾难。Windows Server 2008 系统中新增了“自定义视图”和“应用程序和服务日志”功能，并且在“Windows 日志”中添加了“安装程序”和“转发的事件”查看功能，可极大地提高网络管理员的工作效率。

1. 概述

Windows Server 2008 系统的事件查看器，可以用来查看系统以及网络服务产生的日志记录信息，比 Windows Server 2003 事件查看器的功能强大了许多。以管理员账户登录系统，依次单击“开始”→“管理工具”→“事件查看器”命令，打开如图 9-1 所示的“事件查看器”窗口。

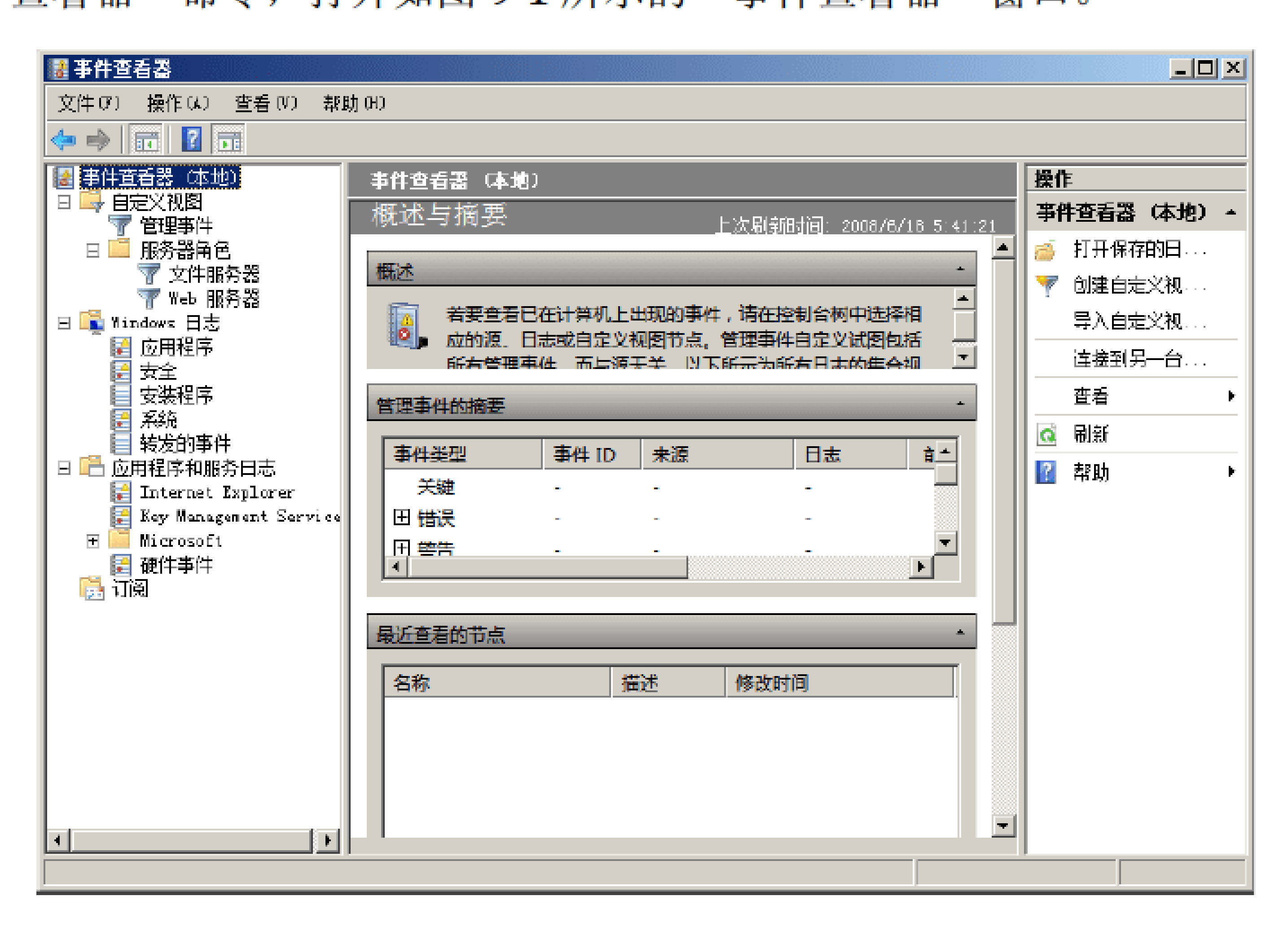


图 9-1 “事件查看器”窗口

(1) Windows 系统日志

Windows Server 2008 系统日志类包括如下 4 种。

- 应用程序日志。应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误。应用程序开发人员决定记录哪些事件。
- 安全日志。安全日志记录诸如有效和无效的登录尝试等事件，以及记录与资源使用相关的事件，如创建、打开或删除文件或其他对象。例如，如果已启用登录审核，登录系统的尝试将记录在安全日志中。
- 系统日志。系统日志包含 Windows 系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。服务器预先确定由系统组件记录的事件类型。
- 安装程序日志。安装程序日志，记录在系统安装或者安装微软公司的产品时，产生的系列事件。如果安装出现错误，可以使用此日志分析出现的问题。

运行 Windows Server 2008 操作系统且配置为域控制器的计算机以另外两种日志记录事件。

- 目录服务日志。目录服务日志包含 Active Directory 服务记录的事件。例如，在目录服务日志中记录服务器和全局编录间的连接问题。
- 文件复制服务日志。文件复制服务日志包含 Windows 文件复制服务记录的事件。例如，在文件复制日志中，记录着文件复制失败和域控制器(利用关于系统卷更改的信息)更新时发生的事件。运行 Windows 并配置为域名系统(DNS)服务器的计算机在其他日志中记录事件。
- DNS 服务器日志。DNS 服务器日志包含 DNS 服务记录的日志。

另外，根据所安装服务的情况，计算机可能会提供其他类型的事件和事件日志。

(2) 应用程序和服务日志

应用程序和服务日志是一种新类别的事件日志，主要是来自单个应用程序或组件的事件。这类日志包括 4 种。

- 管理日志。管理日志可以提供有关如何对事件做出响应的指南。管理事件主要以最终用户、管理员和技术支持人员为目标。管理通道中的事件指示问题以及管理员可以操作的良好定义的解决方案。
- 操作日志。操作日志主要面向 IT 专业人士。操作事件是用于分析和诊断问题或发生的事件，这些事件可以用于基于问题或发生的事件触发工具或任务。
- 分析日志。默认情况下，分析日志和调试日志都为隐藏和禁用状态，用户使用之前必须先将其启用。分析事件是大量发布的事件，这些事件描述程序操作并指示用户干预所无法处理的问题。
- 调试日志。调试日志由开发人员在调试应用程序时使用。

2. 查看事件信息

通过 Windows Server 2008 系统的事件查看器，可以管理服务器角色日志、Windows 系统日志和应用程序日志。事件日志中记录了事件发生的时间、事件来源、用户账户、操作代码及了解详细相关信息的超级链接，管理员通过这些信息可以快速判断服务器或应用程序是否存在故障或安全隐患。在 Windows Server 2008 系统中，事件日志详细信息的基础结构完全符合 XML 架构，且可以访问代表给定事件的 XML。这也是 Windows Server 2008 区别于 Windows Server 2003 的主要方面之一。

① 打开“事件查看器”窗口，在左侧目录栏中展开希望查看和管理的事件日志类别，如“Windows 日志”→“安全”，如图 9-2 所示。系统默认已经启动“预览窗格”功能，即在事件列表中选择时

间后，将自动显示相应预览信息。

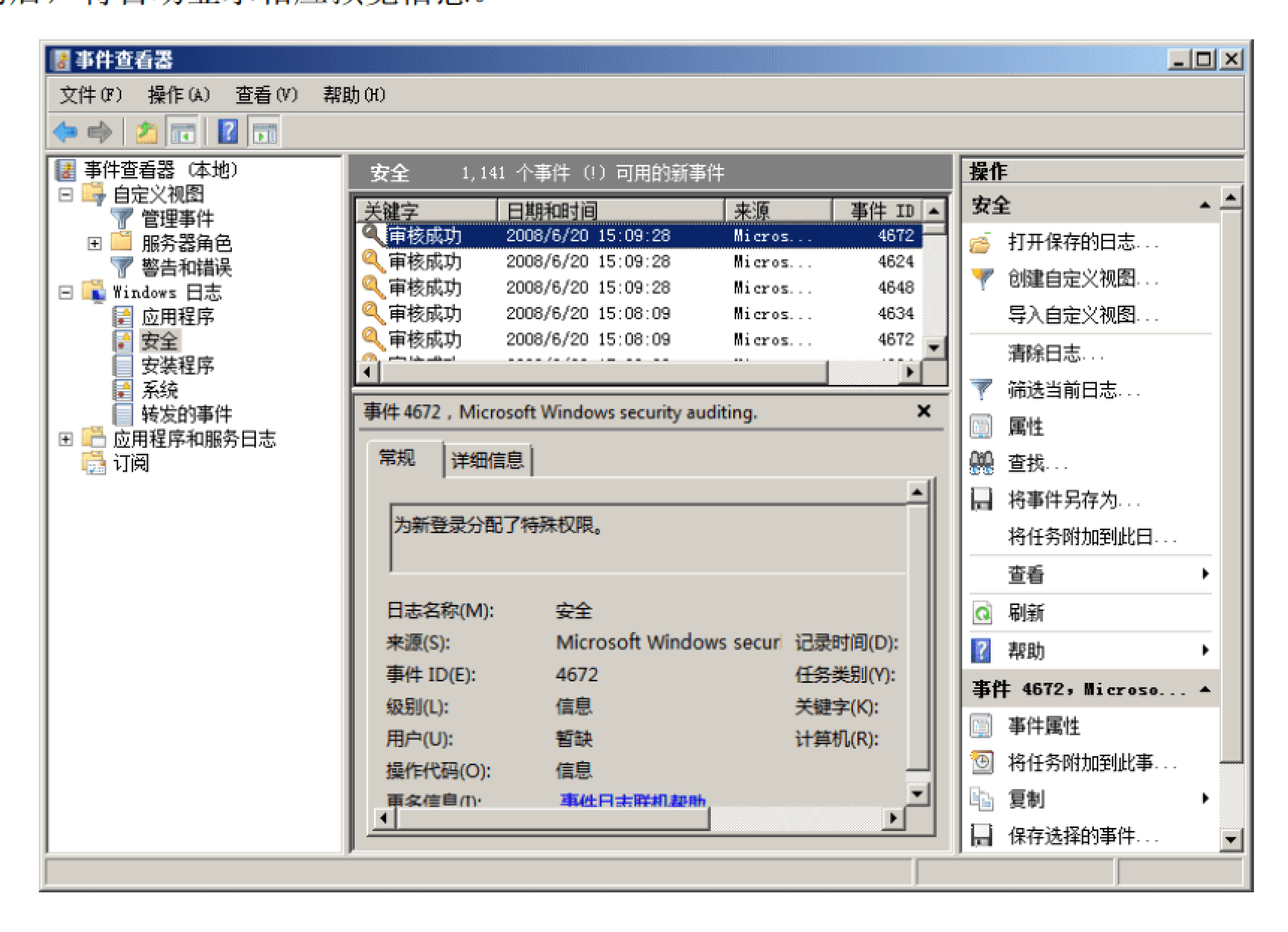


图 9-2　“事件查看器”窗口

② 双击其中的任何一个日志，便可查看详细信息。在日志属性窗口中，可以看到事件发生的日期、事件发生的源、事件发生的种类和 ID，以及事件的详细描述，这些信息有助于帮助系统管理员解决安全问题。如图 9-3 所示为打开一个审核失败的安全事件。



图 9-3　“事件属性”对话框

③ 单击“详细信息”标签切换至如图 9-4 所示的“详细信息”选项卡，系统默认是以“友好视图”方式显示的。

④ 选择“XML 视图”单选按钮，即可以 XML 视图方式显示事件详细信息，如图 9-5 所示。

⑤ 单击“关闭”按钮，关闭“事件属性”对话框即可。

3．将任务附加到事件

Windows Server 2008 系统的事件查看器新增了通知、提醒功能，通过将计划任务附加到指定类型的事件，系统即可自动以某种方式通知用户，如发送 E-mail 邮件、弹出提示信息、开启程序等。可以选择一类系统事件作为关联对象，也可以选择单个事件进行关联。将任务附加到一类事件的具体操作步骤如下。

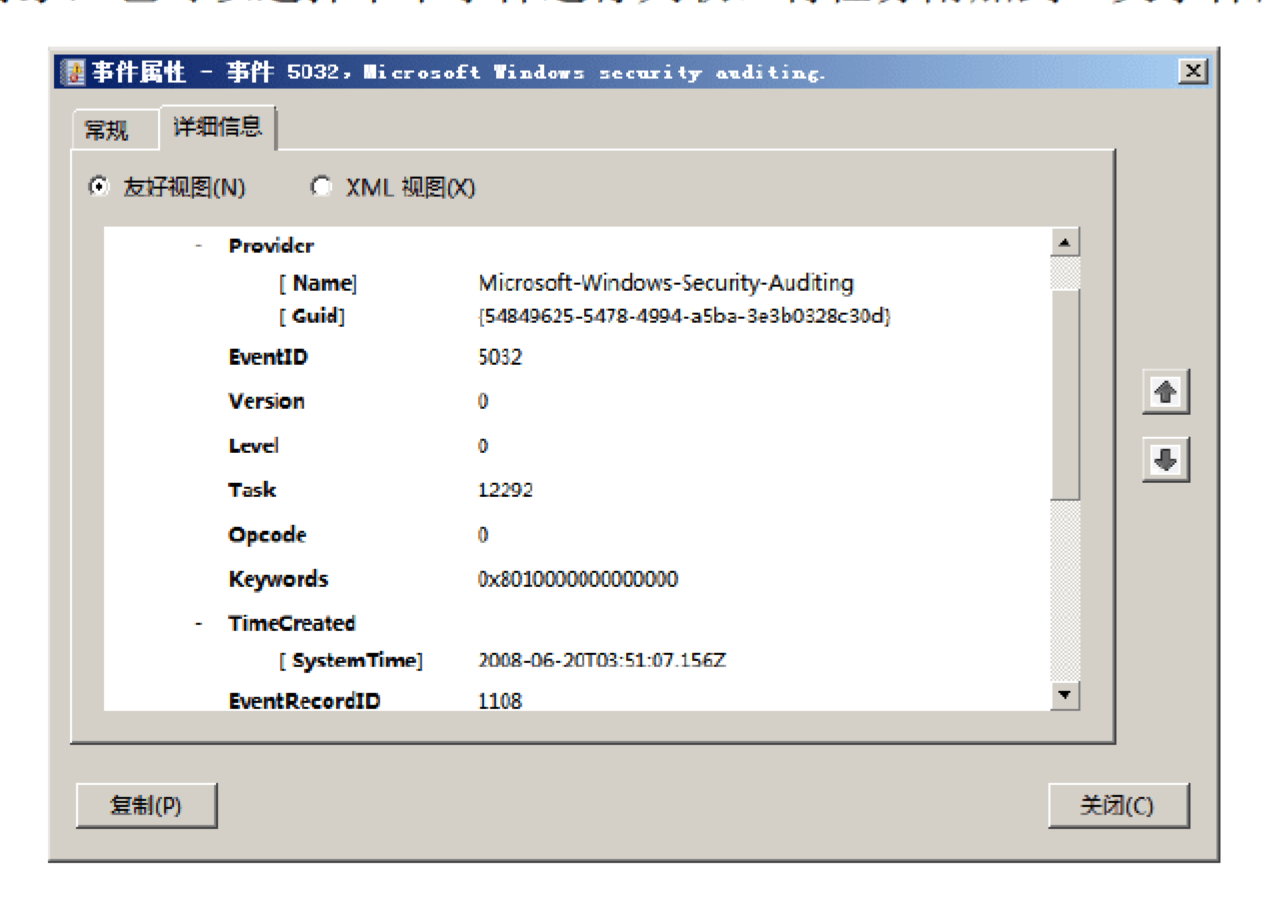


图 9-4　友好视图

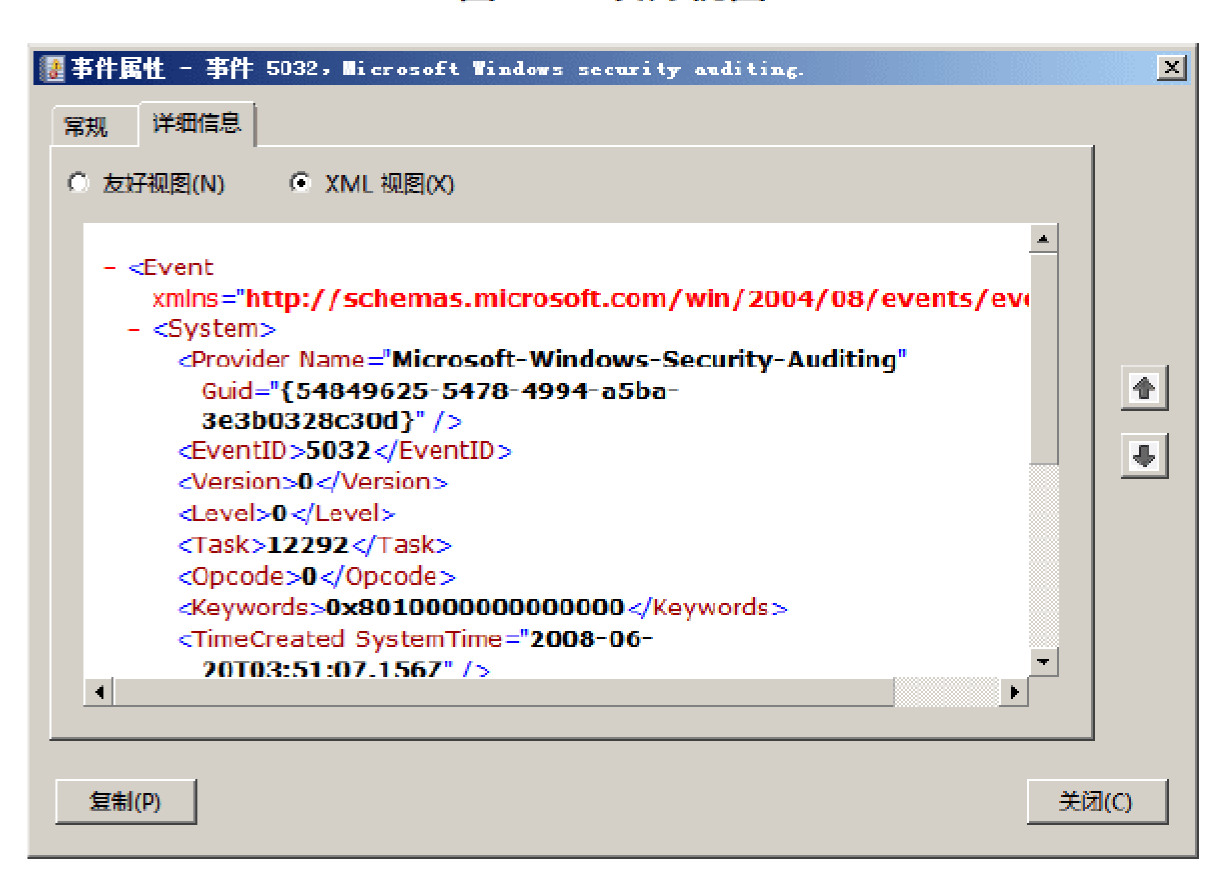


图 9-5　XML 视图

① 在“事件查看器”窗口中，右击“安装程序”(此处以“安装程序”类别的 Windows 事件为例)，并选择快捷菜单中的“将任务附加到事件”命令，启动“创建基本任务向导”，显示如图 9-6 所示的“创建基本任务”界面。使用系统默认名称，并在“描述”文本框中，输入对此基本任务的简单描述，以便区分。

② 单击“下一步”按钮，显示如图 9-7 所示的“登录特定事件时”界面。

③ 单击“下一步”按钮，显示如图 9-8 所示的“操作”界面。定义当事件发生后，希望发生的操作，本例中选择“发送电子邮件”单选按钮。

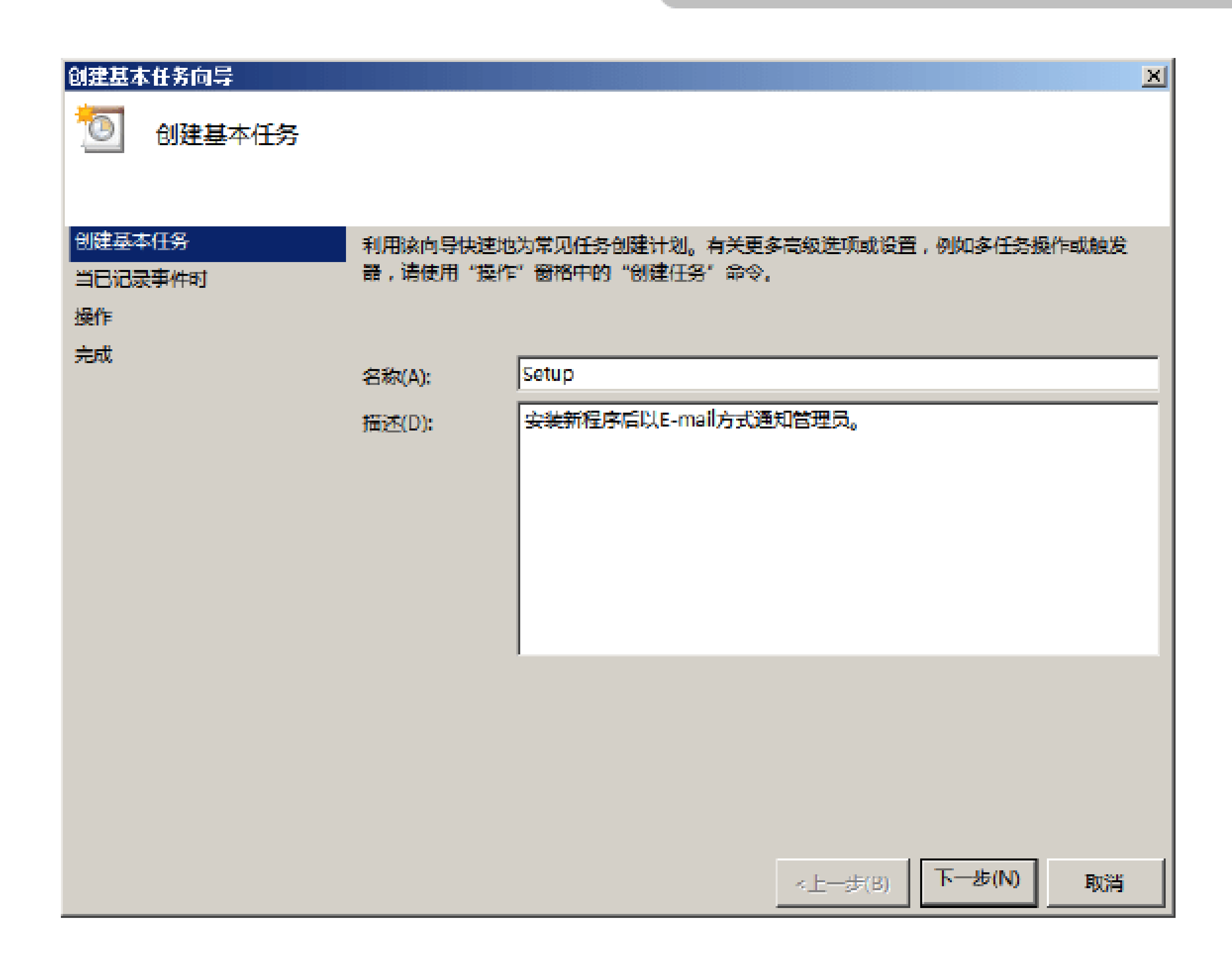


图 9-6　“创建基本任务”界面

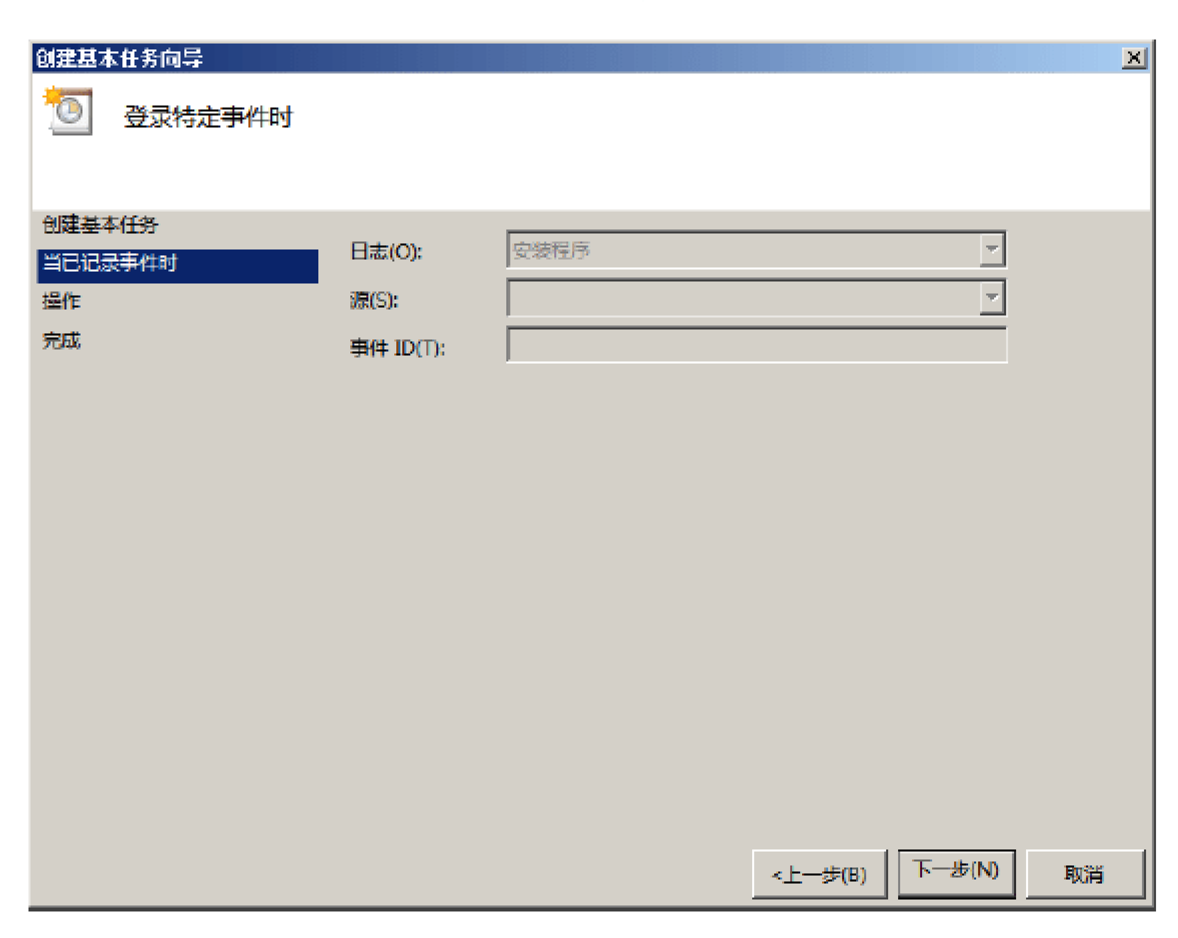


图 9-7　“登录特定事件时”界面

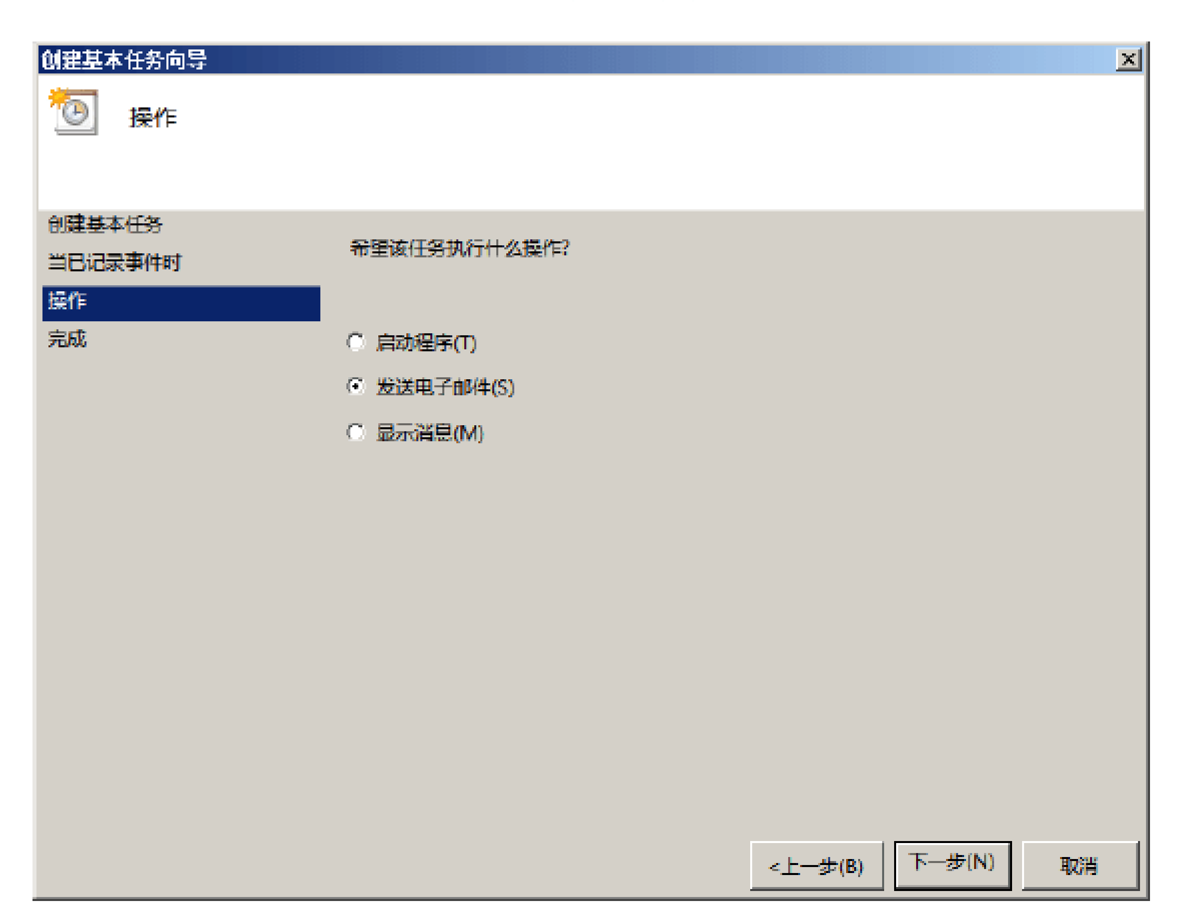


图 9-8　“操作”界面

④ 单击“下一步”按钮，显示如图 9-9 所示的“发送电子邮件”界面。在“发件人”和“收件人”文本框中，输入希望使用的 E-mail 邮箱地址。在“正文”文本框中，可以输入简短的描述信息，告知用户发送此邮件的目的。

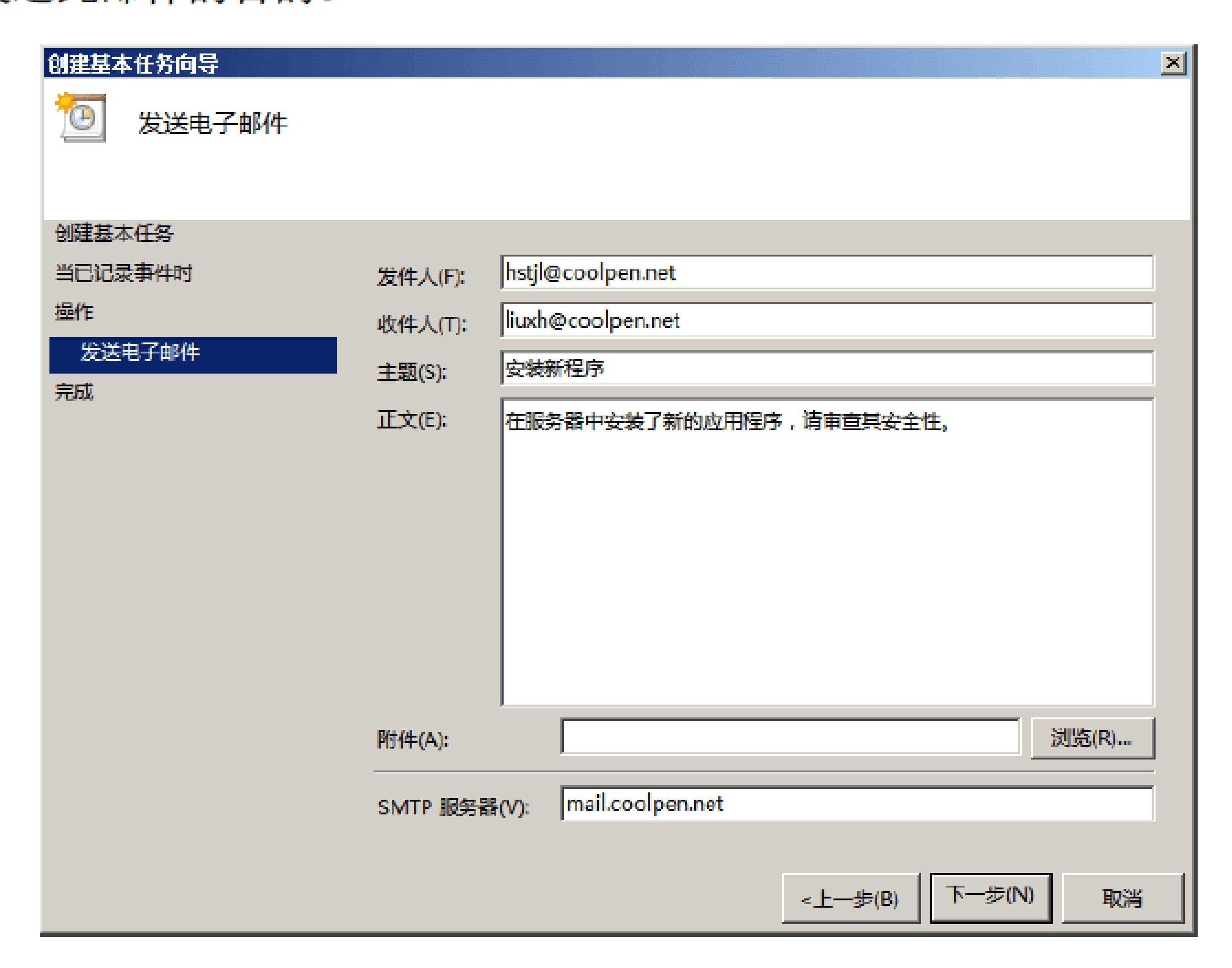


图 9-9 “发送电子邮件”界面

⑤ 单击“下一步”按钮，显示如图 9-10 所示的“摘要”界面，提示当前已作的所有设置。如果选中“当单击‘完成’时，打开此任务属性的对话框”复选框，则关闭“创建基本任务向导”后，可以立即查看和编辑其属性设置。

⑥ 单击“完成”按钮，打开如图 9-11 所示的“事件查看器”提示框，提示计划任务已创建完成，可以在“任务计划程序”中查看和编辑计划的任务。

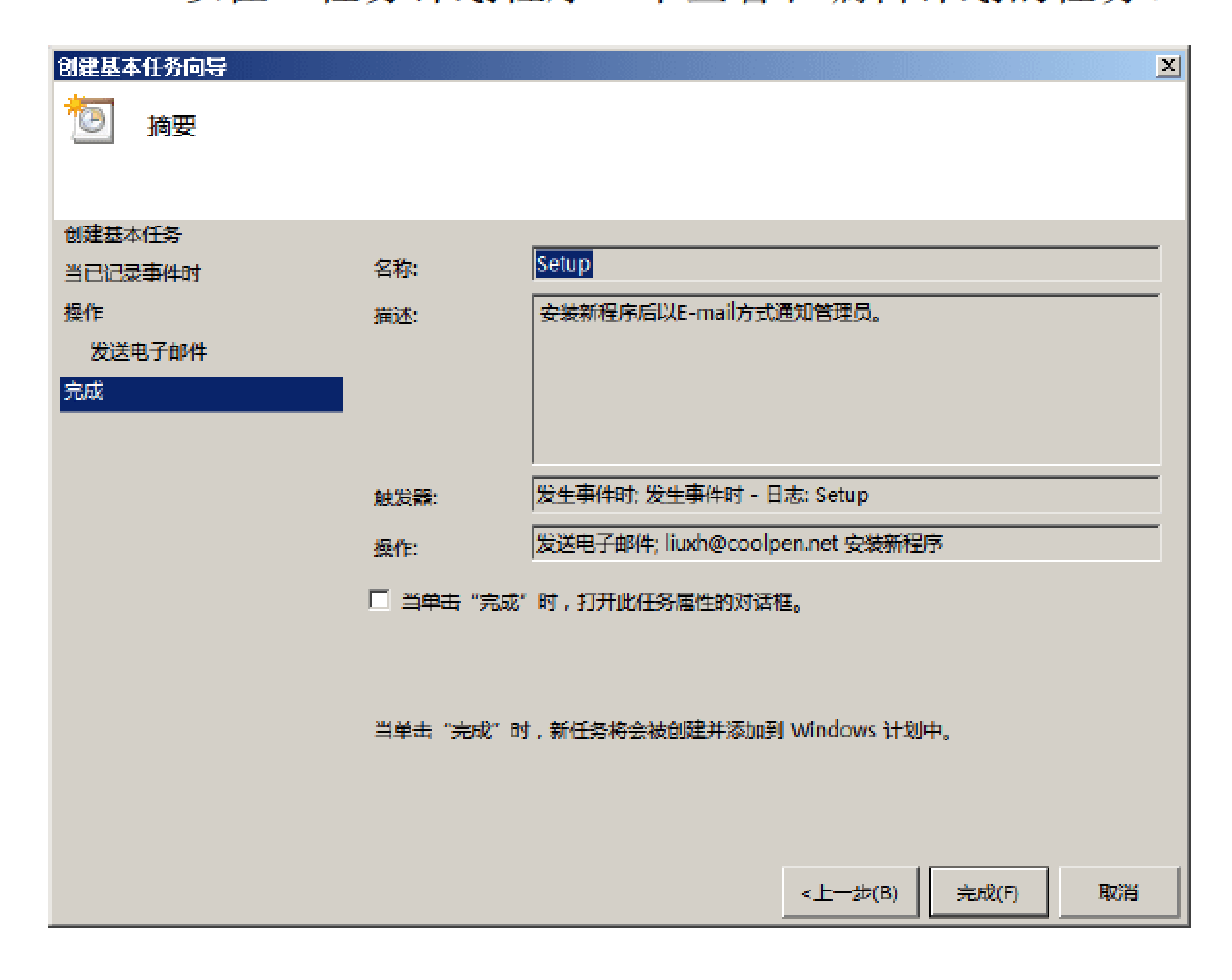


图 9-10 “摘要”界面

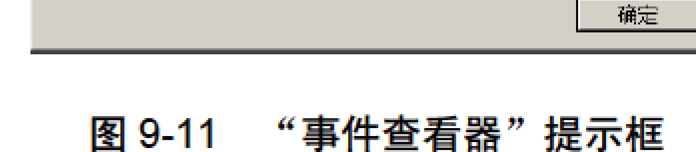


图 9-11 “事件查看器”提示框

⑦ 单击“确定”按钮，关闭对话框即可。



提示： 在 Windows Server 2008 系统中，可以通过依次单击“开始”→“管理工具”→“任务计划程序”命令，打开“任务计划程序”管理器窗口，在此管理员可以对系统中所有的计划任务进行配置和管理。在“事件查看器任务”中创建的任务关联也会显示在这里，如图 9-12 所示。

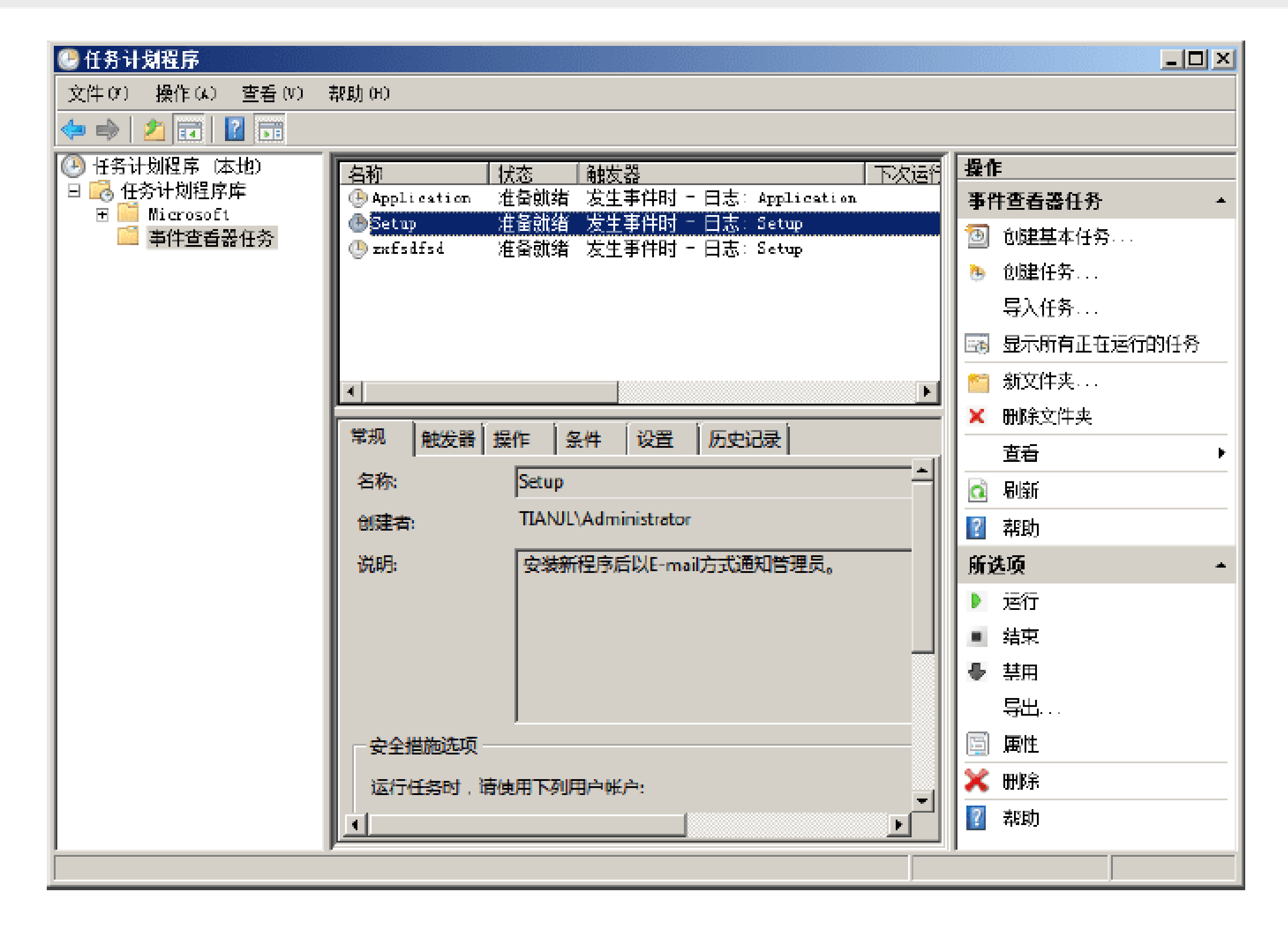


图 9-12 “任务计划程序”窗口

通过“创建基本任务向导”创建的任务关联计划，默认只能设置单一的“触发器”(即执行任务的条件)和“操作”。例如，在“任务计划程序”窗口中，双击已创建的关联任务计划(以 Setup 为例)，打开“Setup 属性(本地计算机)”对话框，在“操作”选项卡中，单击“新建”按钮，打开“新建操作”对话框，在“操作”下拉列表框中，继续选择希望执行的操作类型即可，如图 9-13 所示。

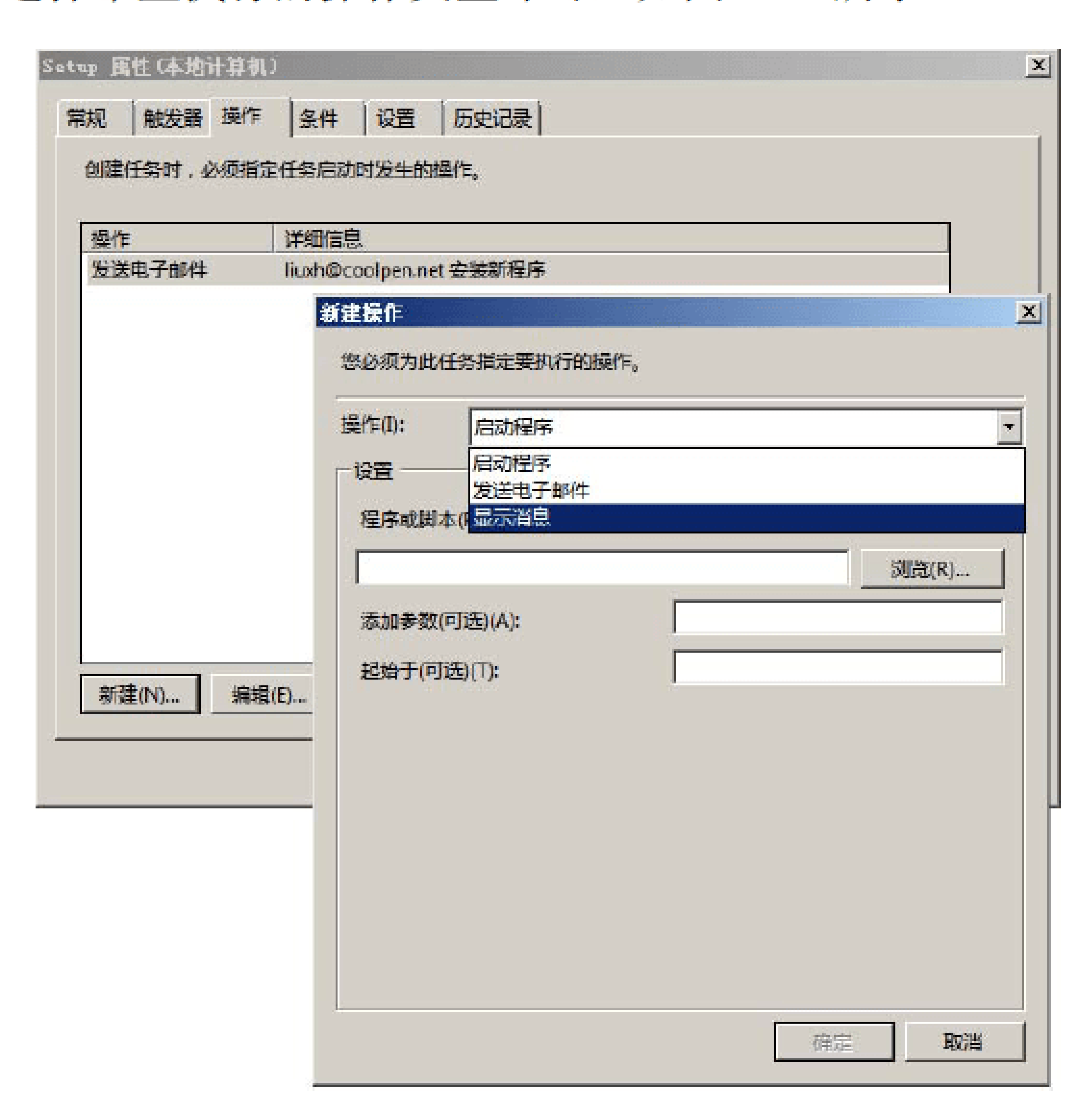


图 9-13 “新建操作”对话框

4．导出和导入日志

如果 Windows 服务器的访问量非常大，则每天产生的日志文件大小也是非常惊人的。尽管安装 Windows 系统和网络服务时，已经选择了安全可靠的日志保存目录，但为了确保日志文件的完整、安全，应适时将其备份至安全性较高的存储介质，如光盘或其他文件服务器等，以免由于系统故障或日志文件自动覆盖，而丢失重要信息。Windows Server 2008 系统中，导出日志文件的操作步骤如下(以 Windows 安全事件日志为例)。

① 在“事件查看器”窗口中展开“Windows 日志”，在导航栏中右击希望导出的时间类型，此处以“安全”事件为例，如图 9-14 所示。

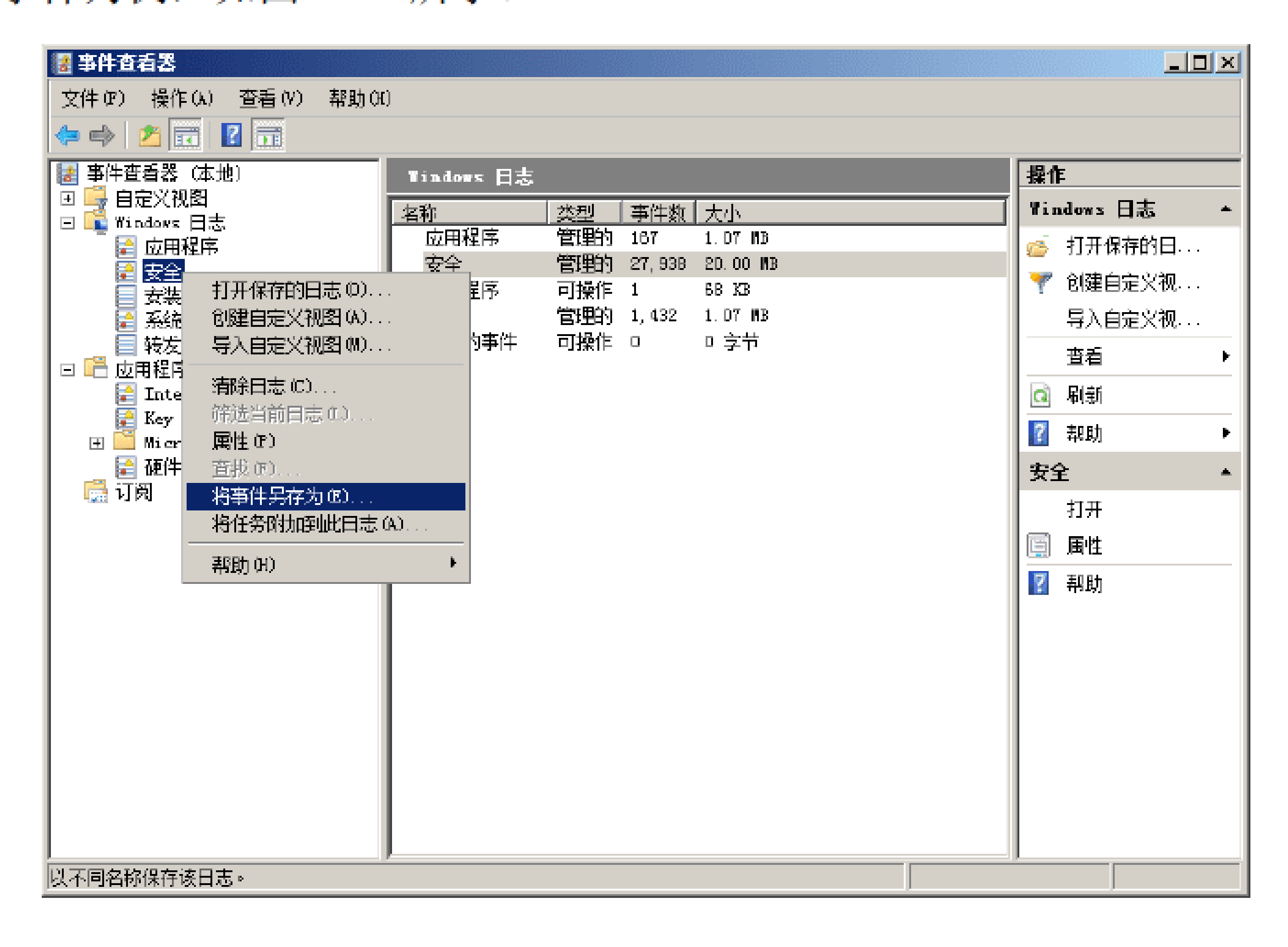
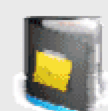


图 9-14　选择希望导出的事件类型

② 选择快捷菜单中的“将事件另存为”命令，打开如图 9-15 所示的“另存为”对话框。如果导出“自定义视图”中的服务器角色日志文件，则需要选择快捷菜单中的“将自定义视图中的事件另存为”命令。在“文件名”文本框中输入日志文件的名称；在“保存类型”下拉列表中，选择导出日志文件的格式，系统默认为*.evtx，此外还支持*.xml、*.txt 和*.csv 格式。其中只有*.evtx 日志文件，才可以在“事件查看器”中重新打开。如果把日志存档为文本(*.txt)或逗号分隔的格式(*.csv)，则可以在文字处理或电子表格之类的其他程序(而不是“事件查看器”)中重新打开日志，建议使用系统默认文件格式。



提示： *.evtx 是 Windows Vista 和 Windows Server 2008 系统的新文件格式，与早期 Windows 系统中的*.evt 文件相同。需要注意的是，*.evtx 文件只能在 Windows Vista 和 Windows Server 2008 系统的“事件查看器”中打开。Windows Server 2008 事件查看器可以兼容 Windows Server 2003 系统中导出的日志文件。

③ 单击“保存”按钮，打开如图 9-16 所示的“显示信息”对话框，系统默认选择“没有显示信息”单选按钮，此时导出日志只能在本地计算机或与本地计算机语言类型相同的其他计算机上打开。如果希望此日志可以在其他系统中查看，则需要选择“显示这些语言的信息”单选按钮，并在列表框中选择与指定计算机系统匹配的语言类型。选中“显示所有可用的语言”复选框，即可显示当前系统支持的所有语言类型。

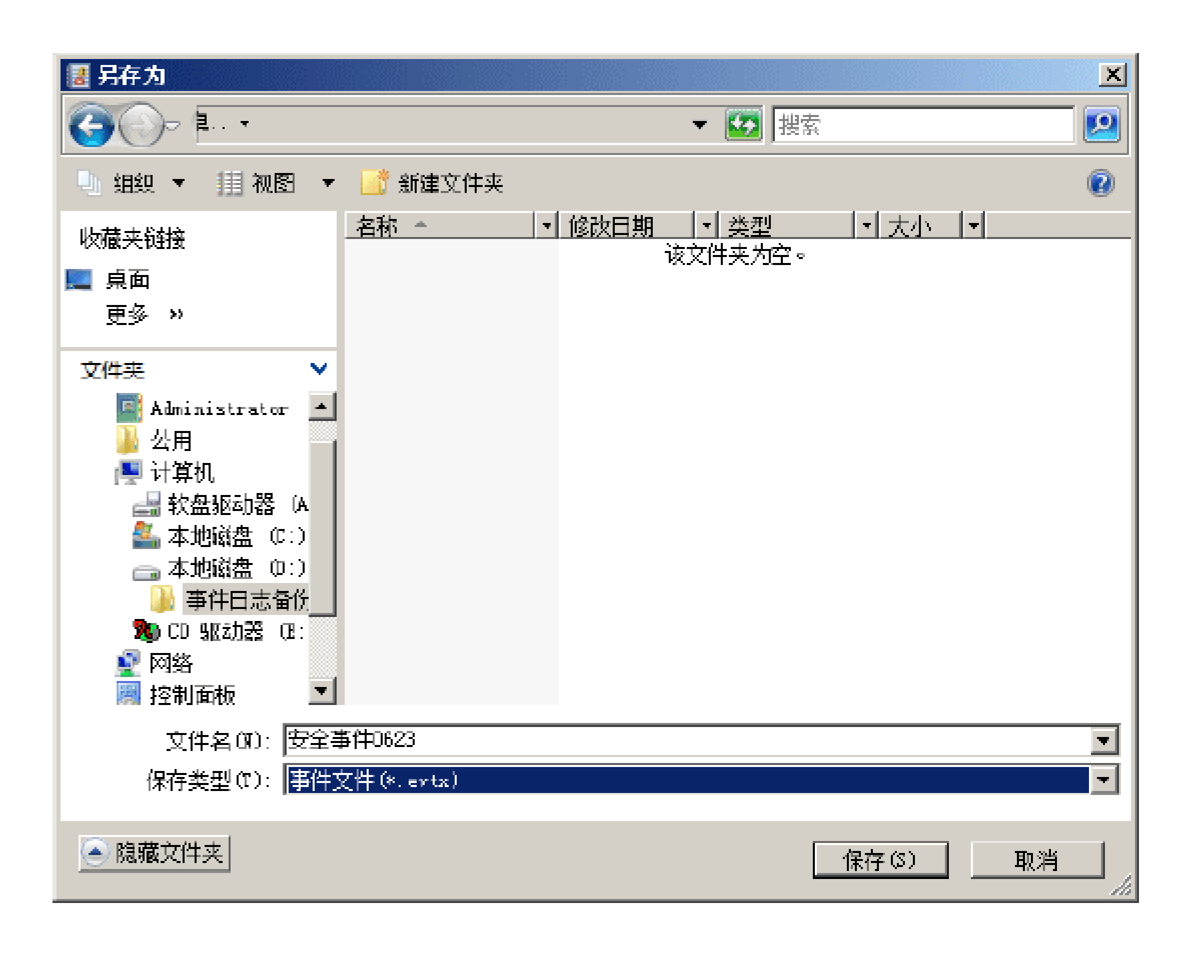


图 9-15　“另存为”对话框

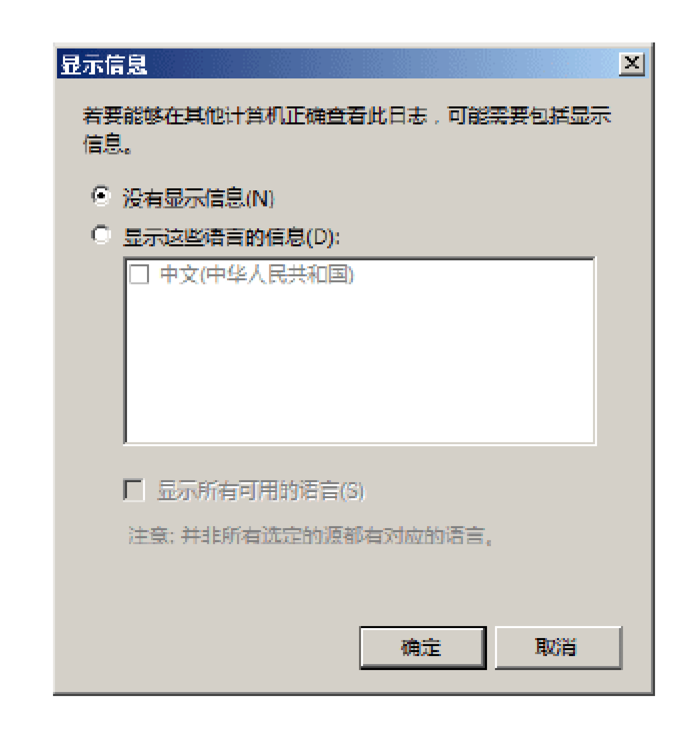


图 9-16　“显示信息”对话框

④　单击“确定”按钮，保存日志。

⑤　在其他计算机的“事件查看器”窗口中，右击导航栏中的任意项目，并选择快捷菜单中的“打开保存的日志”命令，打开如图 9-17 所示的“打开保存的文件”对话框，选择希望导入的目标文件即可。

⑥　单击“打开”按钮，打开如图 9-18 所示的“打开保存的文件”对话框。默认将在“事件查看器”导航栏中创建“保存的日志”项目，用于保存所有导入事件文件。选中“所有用户”复选框，则本地计算机上的所有用户均可通过事件查看器查看当前文件，取消选中则只有本地管理员账户可以查看该文件。

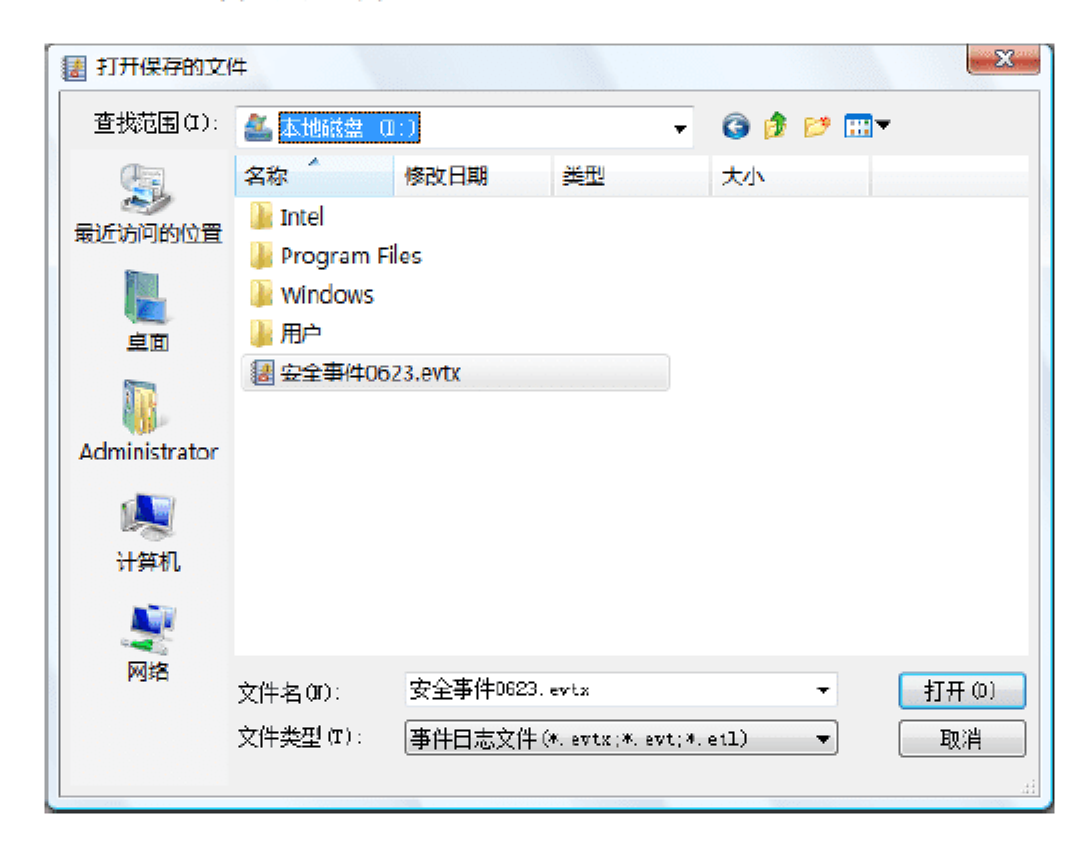


图 9-17　“打开保存的文件”对话框

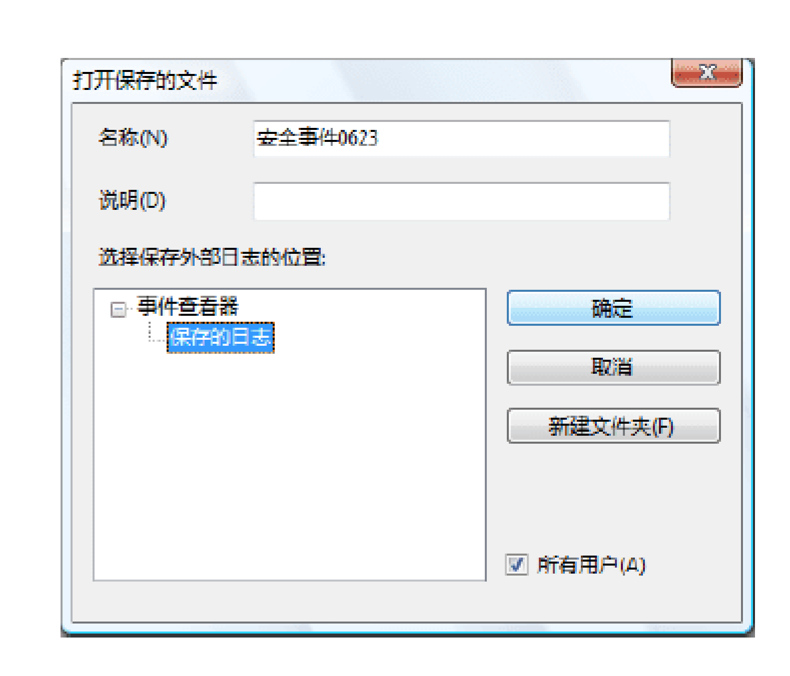


图 9-18　“打开保存的文件”对话框

⑦　单击“确定”按钮，即可将其添加到“事件查看器”窗口中，如图 9-19 所示。

5．订阅事件

Windows Server 2008 系统的事件查看器可以订阅来自其他 Windows 系统(Windows Vista 或 Windows Server 2008)的事件日志，通过它管理员可以轻松做到集中分析和监控计算机的状态。订阅功能依赖于 Windows 远程管理(WinRM)服务和 Windows 事件收集器(Wecsvc)服务，这两项服务必须在参与转发和收集过程的计算机上运行，目前只有运行 Windows Server 2008 和 Windows Vista 操作系统的计算机支持此

功能。

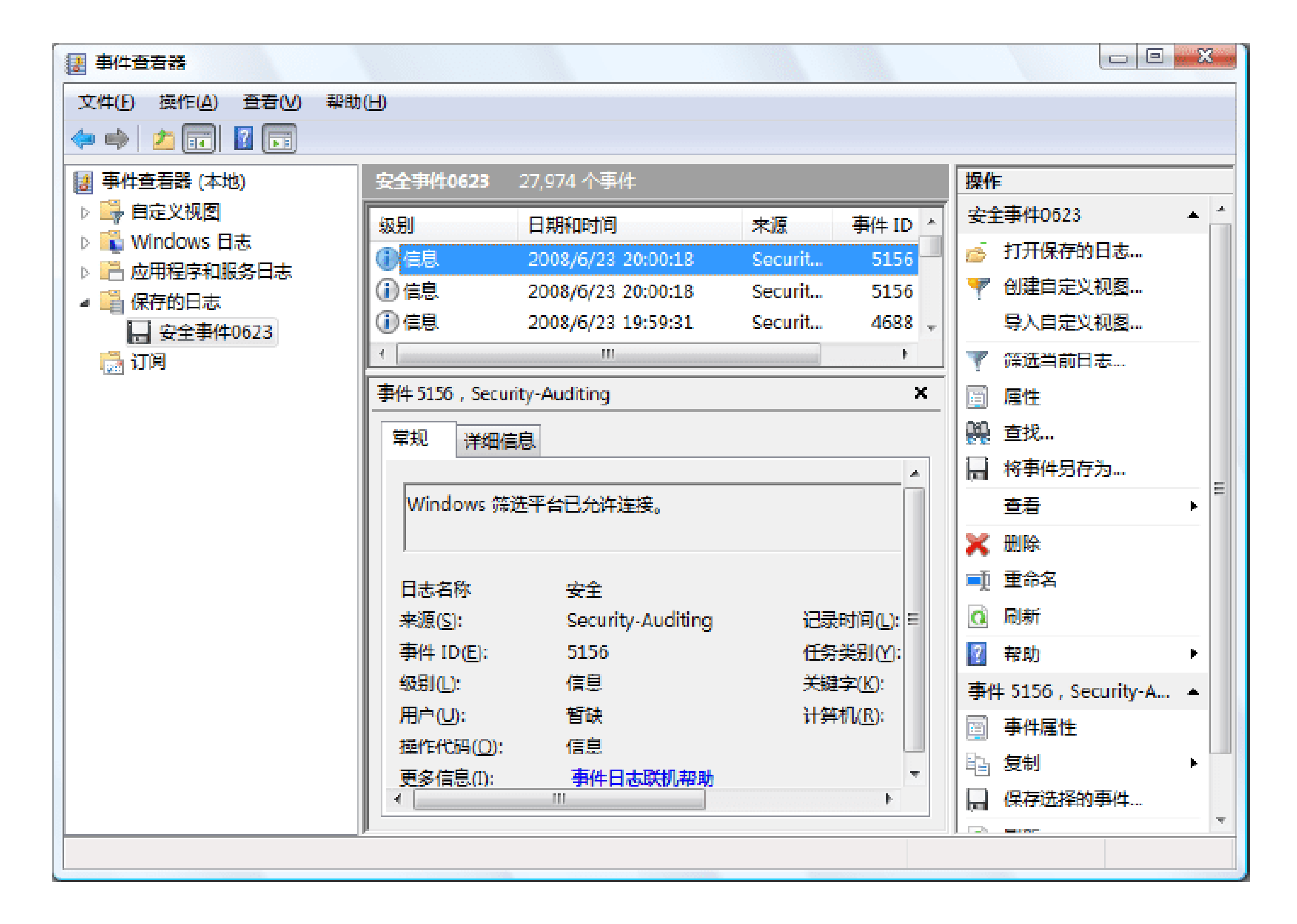


图 9-19　导入的事件日志

(1) 配置源计算机

所谓源计算机就是指事件的真正来源，此处以 Windows Vista 系统为例，需要在源计算机上开启远程管理功能，即允许收集服务器通过网络登录并管理该计算机。需要注意的是，源计算机和事件收集服务器必须隶属于同一域，或建立信任关系的不同域中。主要操作步骤如下。

① 以管理员登录系统，在命令提示符窗口中，输入如下命令：

```
winrm quickconfig
```

按 Enter 键执行，显示如图 9-20 所示的结果，提示目前该计算机没有设置成为允许远程访问。执行更改后，即可接受远程访问，是否继续。

② 输入“Y”并按 Enter 键执行，表示确认更改，显示如图 9-21 所示的结果。

图 9-20　是否允许远程访问

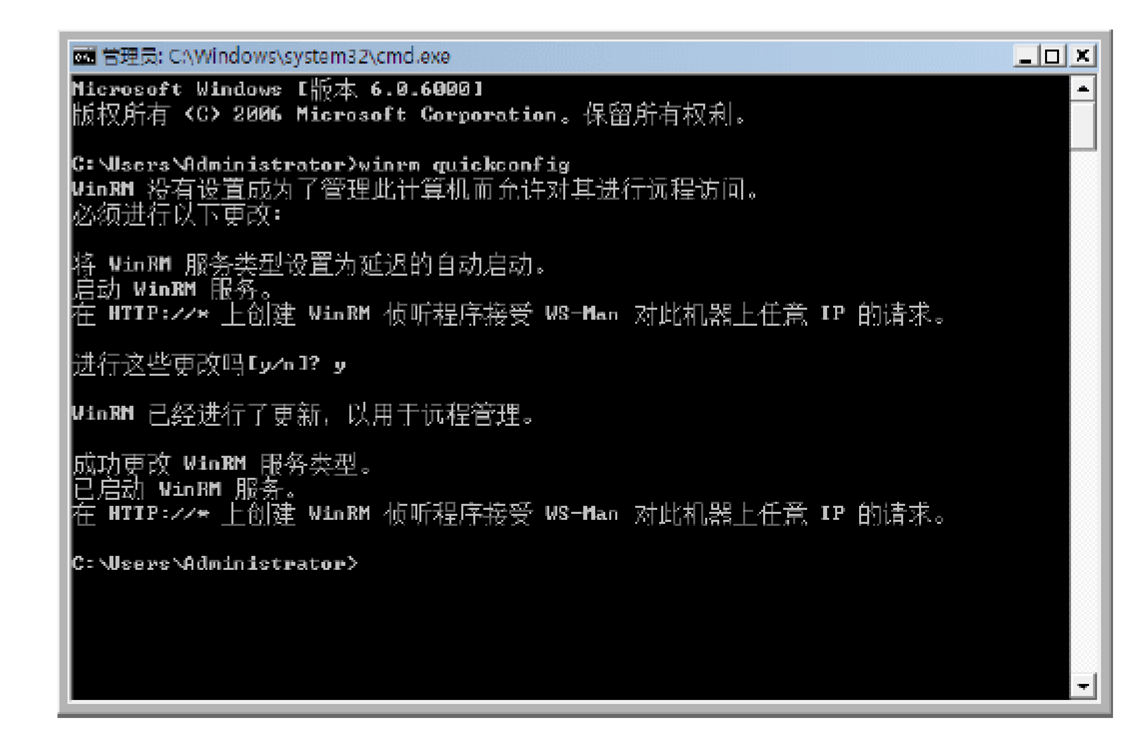


图 9-21　启动 WinRM 服务

③ 将事件收集服务器的计算机账户添加到本地计算机的 Administrators 组中。依次单击“开始”→“控制面板”→“管理工具”→“计算机管理”命令，打开“计算机管理”窗口，展开“系统工

具”→“本地用户和组”→“组”项目，双击 Administrators 打开如图 9-22 所示的“Administrators 属性”对话框。

④ 单击“添加”按钮，打开“选择用户、计算机或组”对话框。默认情况下，只能向该组中添加用户或组对象。单击“对象类型”按钮，打开“对象类型”对话框，选中“对象类型”列表框中的“计算机”，如图 9-23 所示。

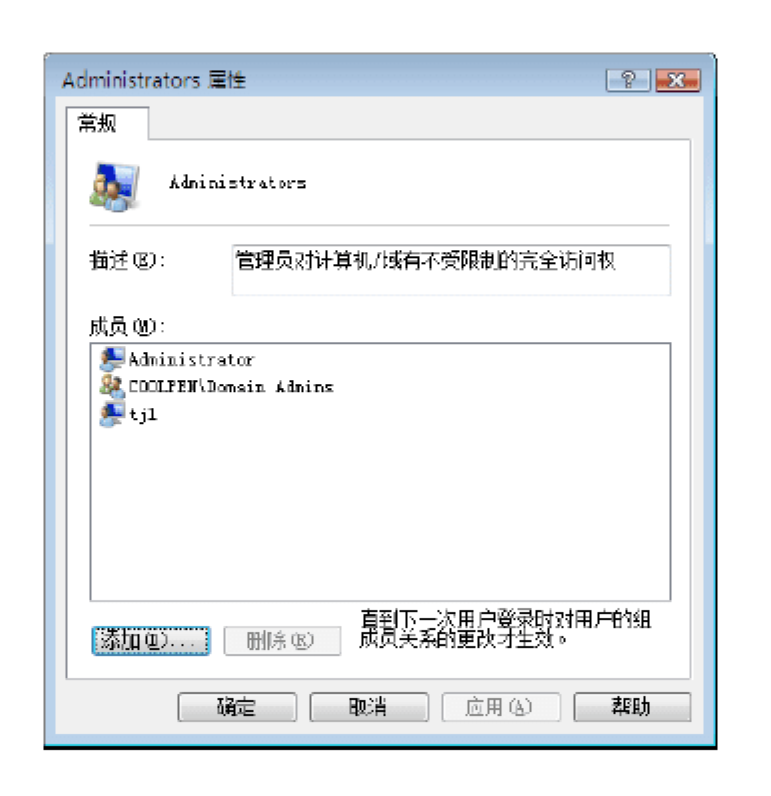


图 9-22　“Administrators 属性”对话框

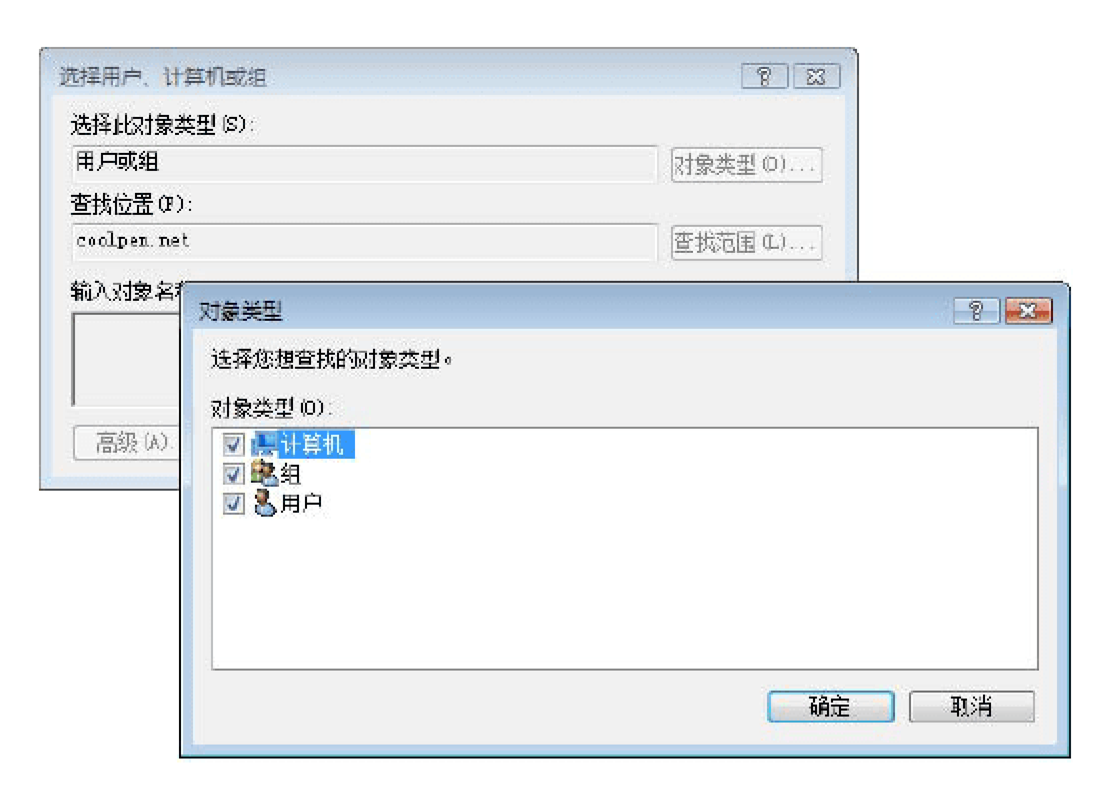


图 9-23　“对象类型”对话框

⑤ 单击“确定”按钮，返回“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入事件收集服务器的主机名，如图 9-24 所示。也可以单击“高级”按钮，从指定位置的所有对象中搜索希望添加的服务器。

⑥ 单击“确定”按钮，将其添加至 Administrators 组成员列表中，如图 9-25 所示。

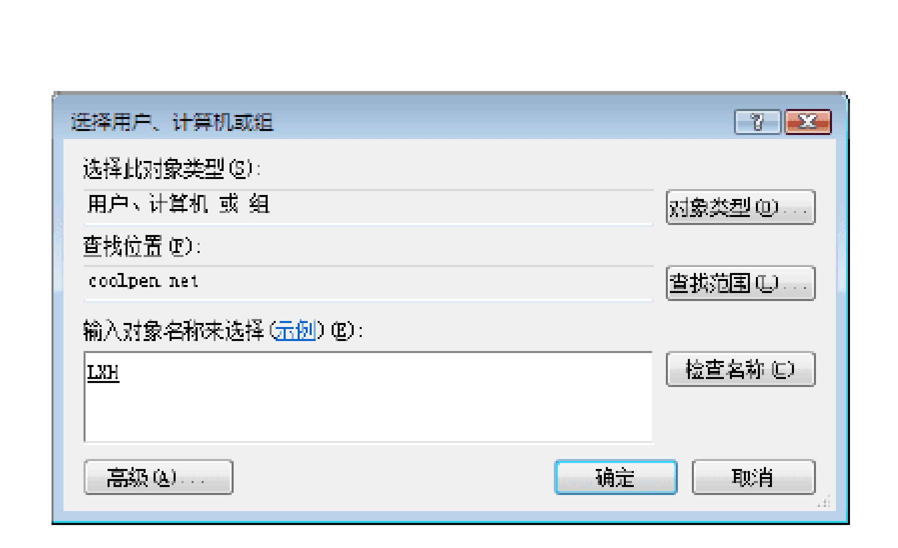


图 9-24　“选择用户、计算机或组”对话框

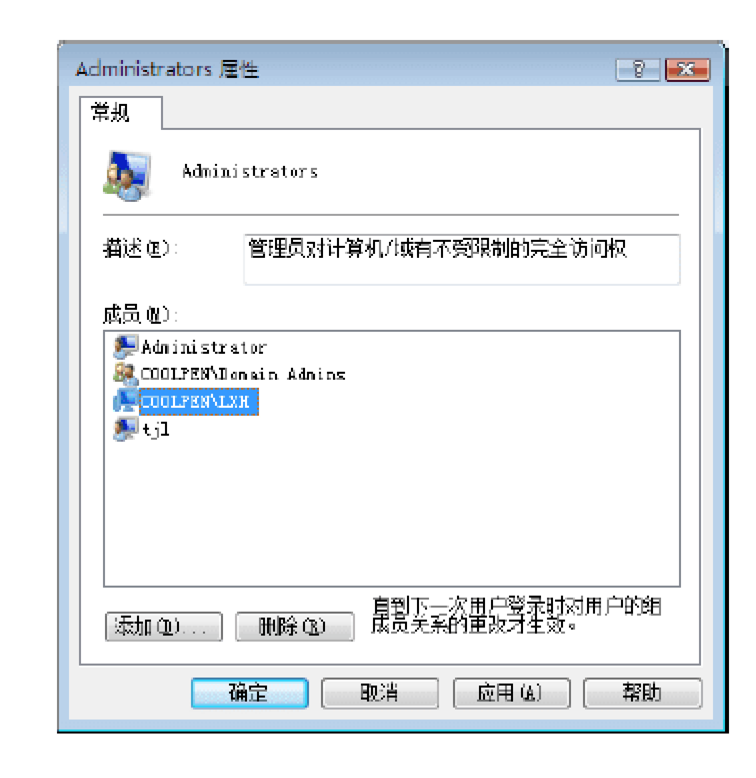


图 9-25　成功添加到成员列表中



提示：重复上述操作，可以配置多台源计算机。

(2) 配置收集服务器

如果指定了较多的源计算机，则运行过程中可能产生大量的日志文件，如果源计算机是应用程序服务器，则数据量更大。为确保事件日志的安全，建议采用单独的服务器作为收集服务器。

① 打开“管理员：命令提示符”窗口，输入如下命令：

```
wecutil qc
```

按 Enter 键执行，显示如图 9-26 所示的结果，提示是否更改服务启动模式。



提示： wecutil qc 命令主要用于快速配置事件收集服务器，其中 qc 是 quick-config 的缩写。确认执行该命令后，主要完成如下操作。
如果已禁用 ForwardedEvents(转发的事件)通道，则启用该通道。
将 Windows 事件收集器服务设置为延迟启动(仅适用于 Windows Vista 和更新的 Windows 系统)。
如果 Windows 事件收集器服务未运行，则启动该服务。

② 输入“Y”并按 Enter 键，确认执行更改，显示如图 9-27 所示的结果，事件收集服务器配置成功。

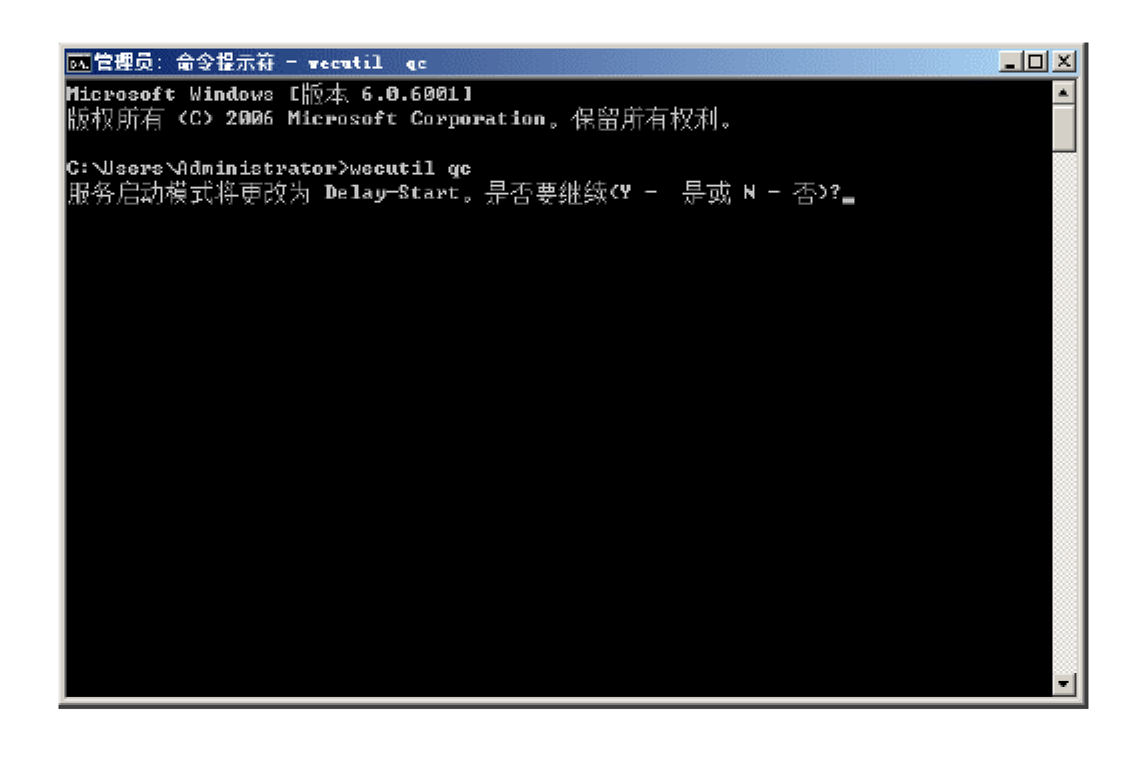


图 9-26 是否更改服务器启动模式

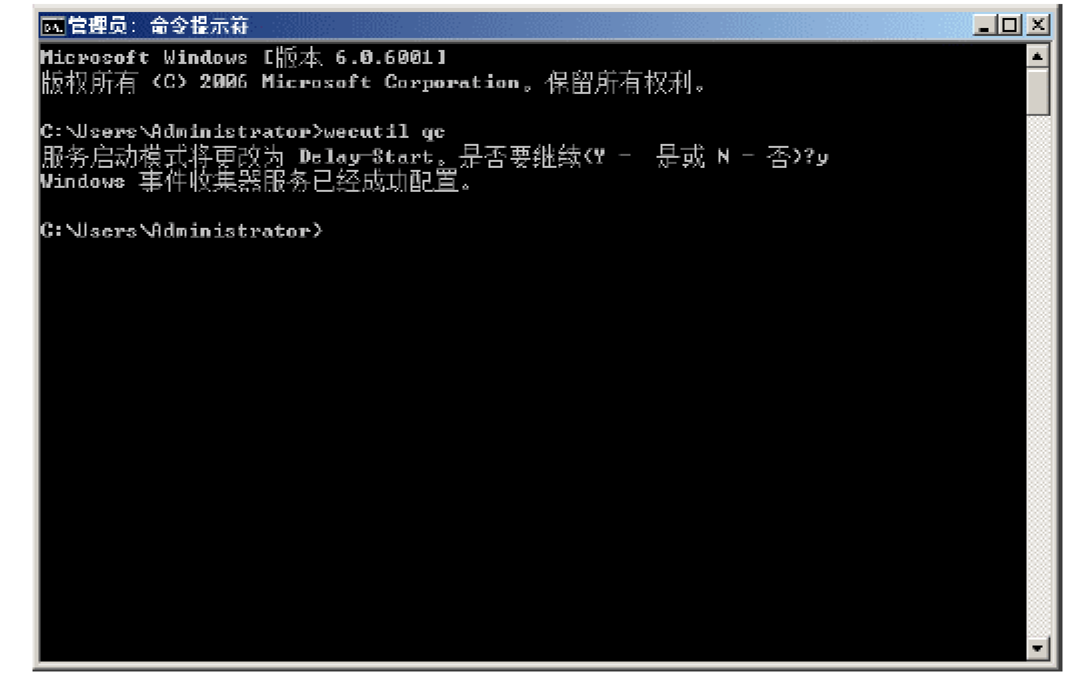
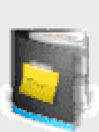


图 9-27 成功配置事件收集服务器



提示： 如果要指定“最小化带宽”或“最小化滞后时间”的事件传递优化，则还必须在收集器计算机上运行 winrm quickconfig 命令。

(3) 创建订阅

若要在事件收集服务器上接收来自其他计算机的事件日志，必须创建一个或者多个事件订阅，在源计算机和事件收集服务器上做好上述准备工作之后，即可开始配置事件订阅。主要操作步骤如下。

① 在事件收集服务器上打开“事件查看器”窗口，并在导航栏中选择“订阅”，如图 9-28 所示。



提示： 默认情况下，Windows Vista 和 Windows Server 2008 系统均为启动事件收集所需的系统服务。未做好事件收集服务器的准备工作之前，选择“订阅”项目时，会弹出如图 9-29 所示“事件查看器”对话框。

② 在“操作”栏中单击“创建订阅”链接，打开如图 9-30 所示的“订阅属性”对话框。在“订阅名称”文本框中，输入该订阅的名称；在“说明”文本框中可输入相关的说明性文字，以便区分；“目标日志”用于保存所收集事件的目录，默认目录为“Windows 日志”中的“转发的事件”。

③ 在“订阅类型和源计算机”选项组中，选择“收集器已启动”单选按钮，并单击“选择计算机”按钮，打开“计算机”对话框，单击“添加域计算机”按钮，打开如图 9-31 所示的“选择计算机”对话框。在“输入要选择的对象名称”文本框中，输入域中源计算机的主机名。可以同时输入多个，彼此之间以分号“；”隔开；也可以单击“高级”按钮，在所有目录对象中查找。

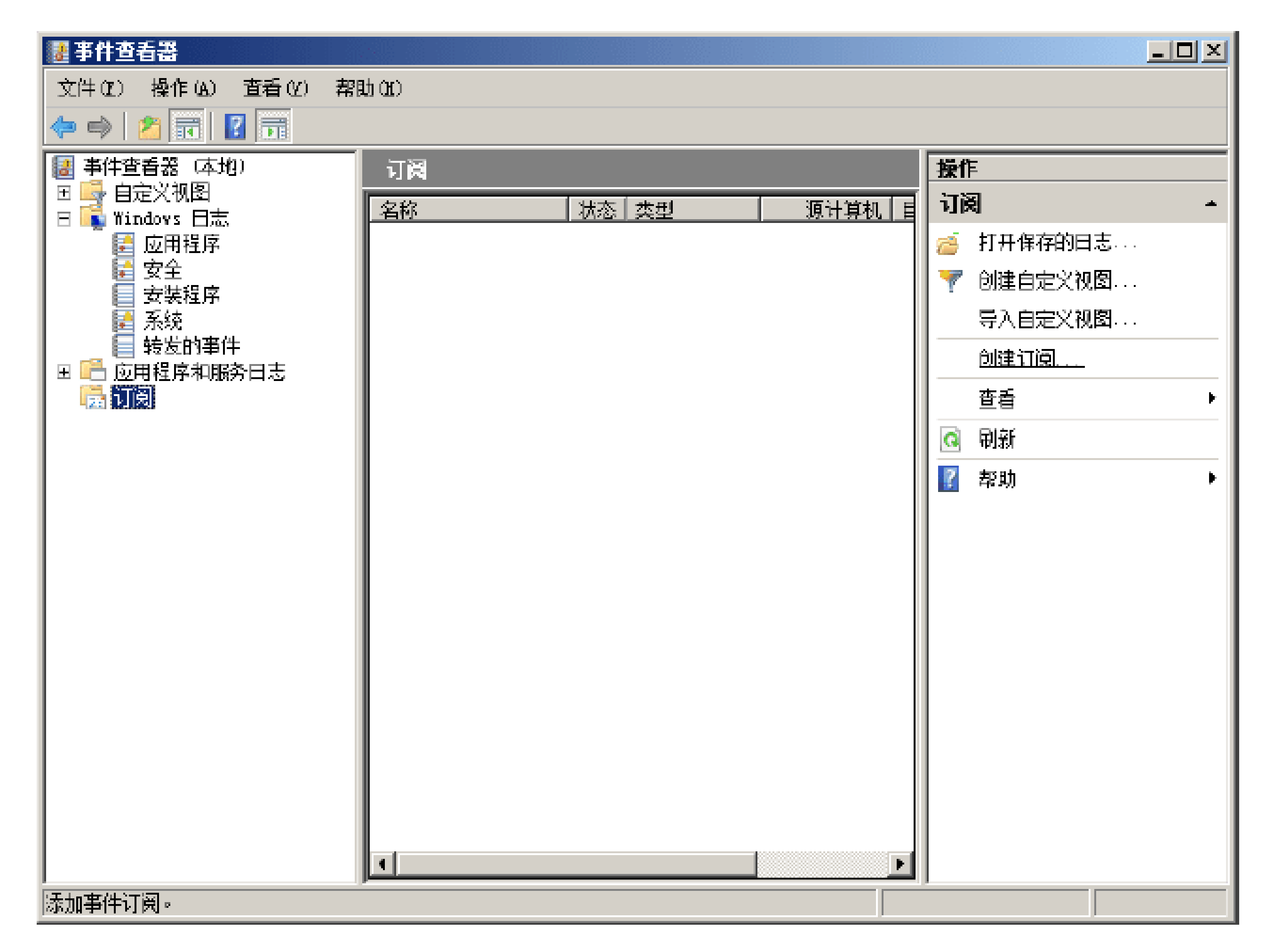


图 9-28 “事件查看器”窗口

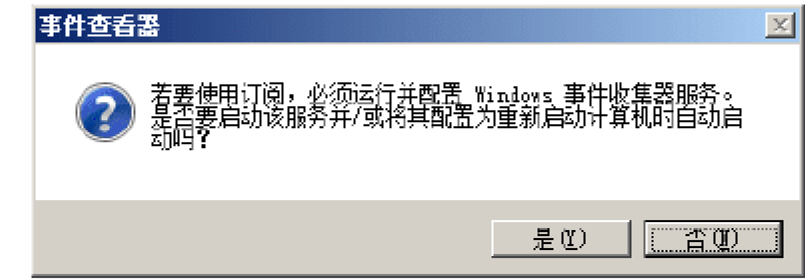


图 9-29 “事件查看器”对话框

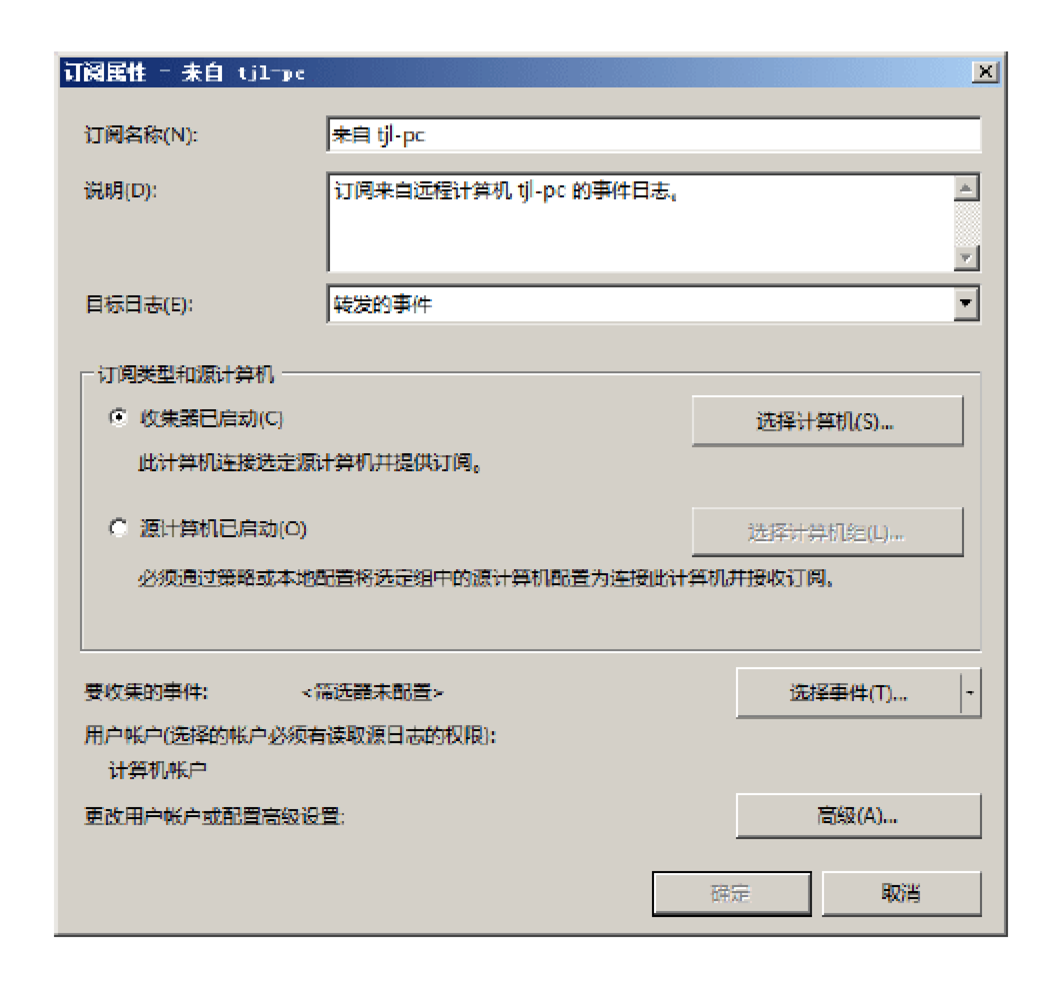


图 9-30 “订阅属性”对话框

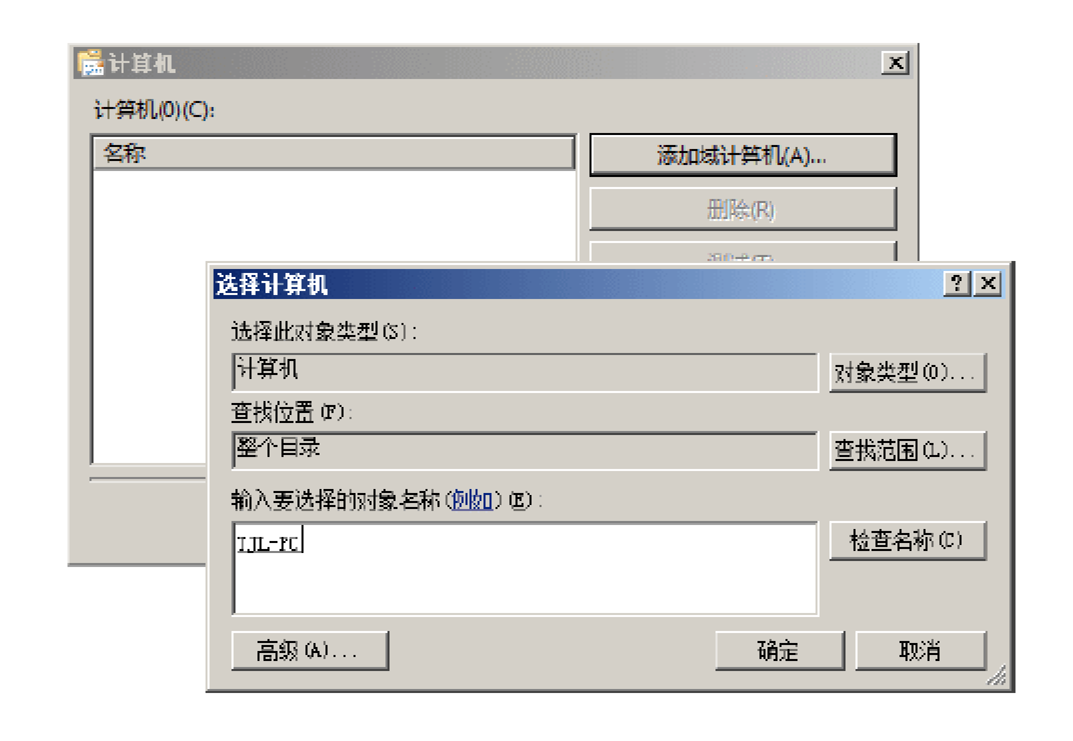


图 9-31 “选择计算机”对话框

④ 单击“确定”按钮，将所选计算机添加到“计算机”列表中，如图 9-32 所示。

⑤ 为确保事件收集服务器和所选源计算机之间的连接正常，可以在“计算机”列表中，选中源计算机名称并单击“测试”按钮，如果显示如图 9-33 所示的“连接测试成功”的结果，则表示连接正常。

⑥ 连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 9-34 所示的“查询筛选器”对话框。在“记录时间”下拉列表框中选择希望收集的事件产生的时间和日期；在“事件级别”选项区域选择被收集事件的级别；选择“按日志”单选按钮，并在“事件日志”下拉列表中，选择事件类型。需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

⑦ 单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 9-35 所示的“高级订阅设置”对话框。由于已经将事件收集服务器的计算机账户添加到了源计算机的 Administrators 组中，所以选择“计算机账户”单选按钮即可。

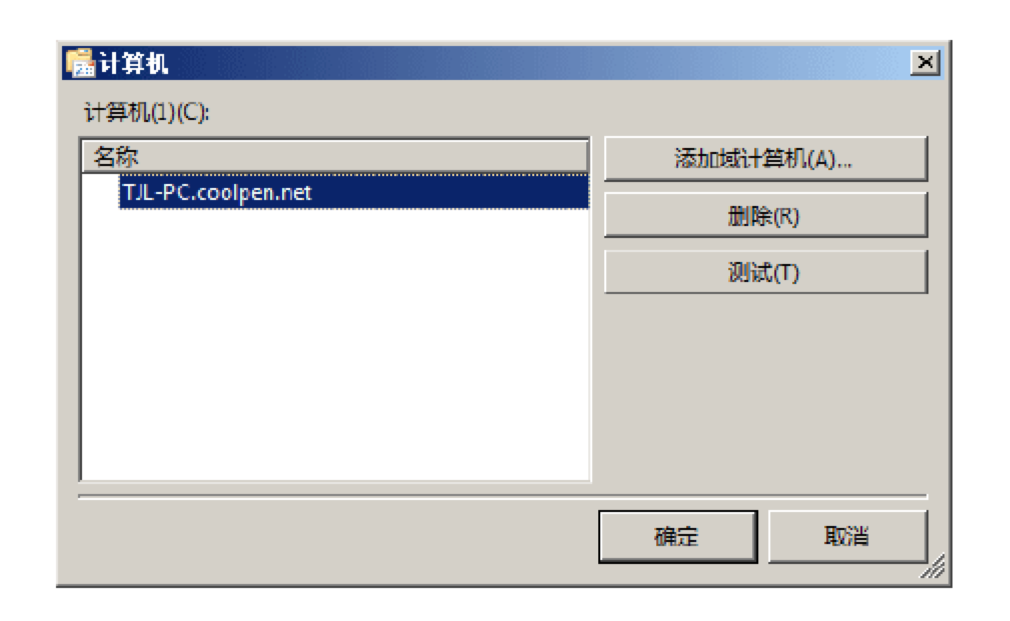


图 9-32 “计算机”对话框



图 9-33 “连接测试成功”对话框

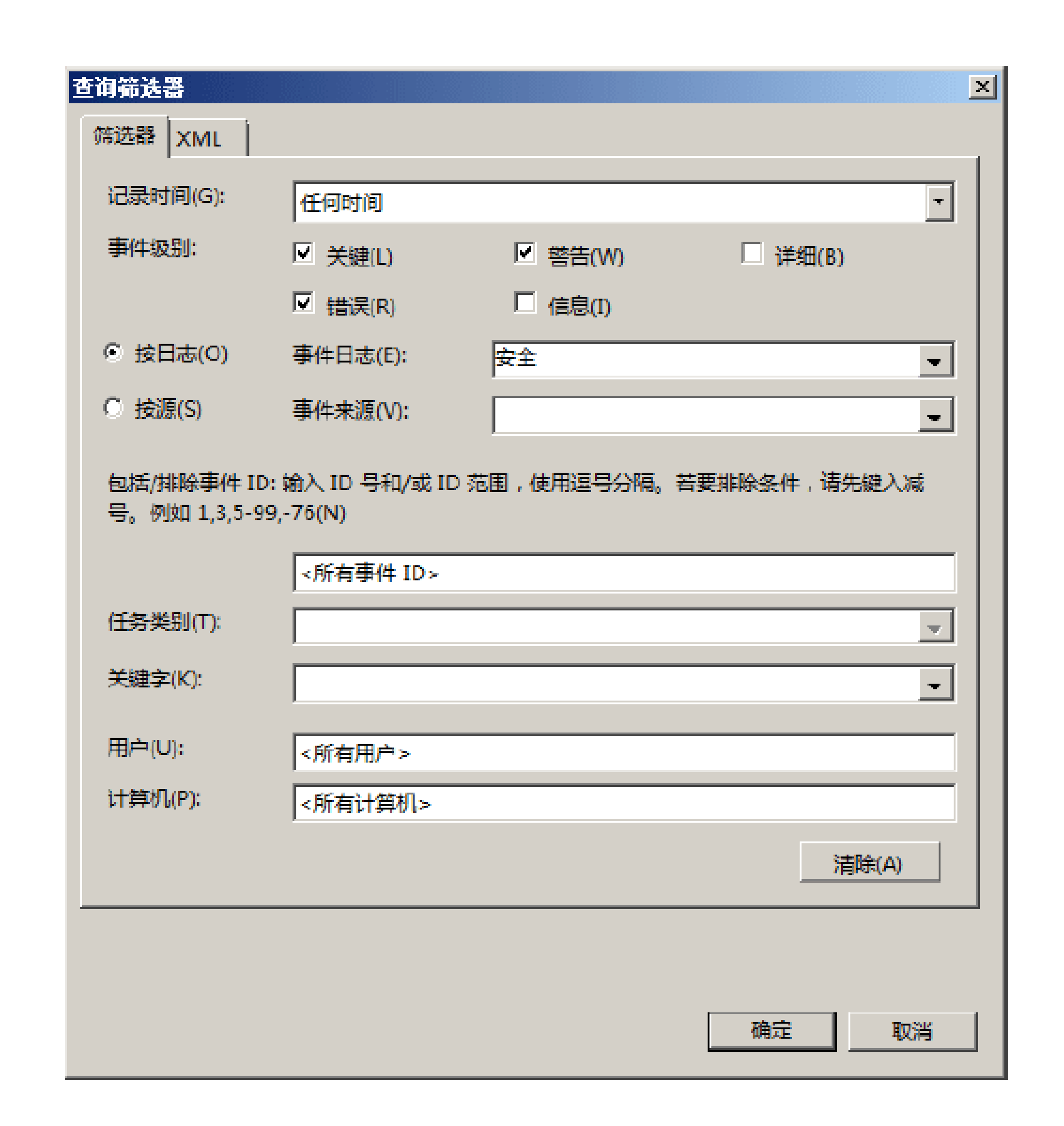


图 9-34 “查询筛选器”对话框

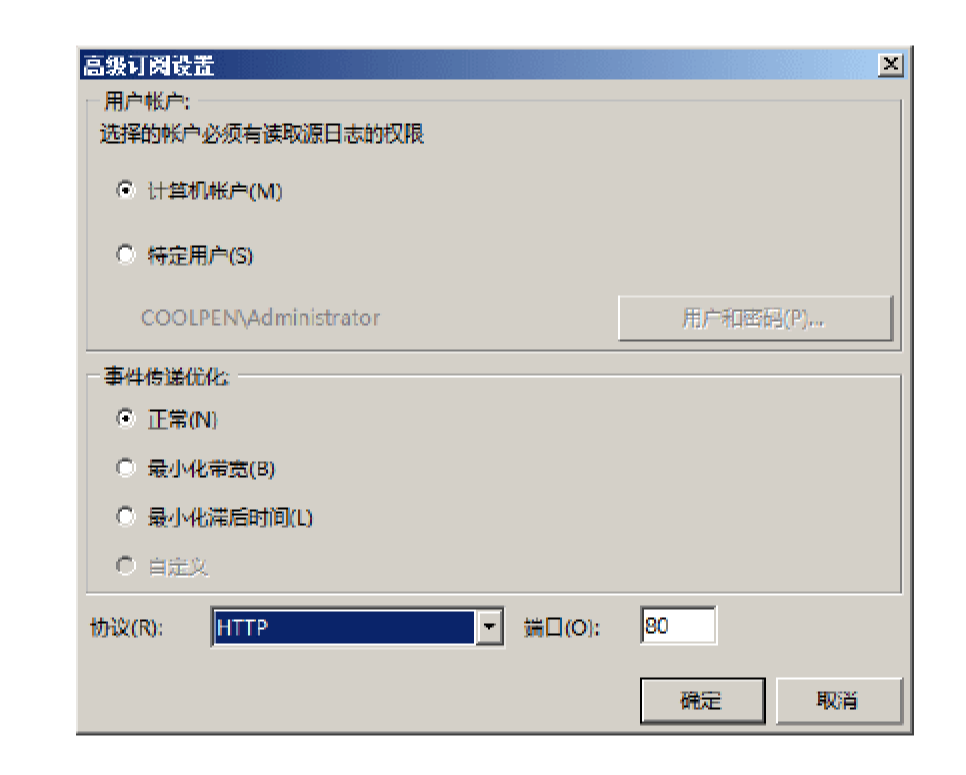


图 9-35 “高级订阅设置”对话框

对“高级订阅设置”对话框中一些选项说明如下。

- 特定用户。若要指定用于管理收集事件的过程的账户，则可以选择“特定用户”单选按钮，然后单击“用户和密码”按钮，打开如图 9-36 所示的“订阅源的凭据”对话框，输入账户的用户名和密码即可。
- 事件传递优化。在这里用户可以根据网络连接状况设置适当的优化措施。例如，如果不希望占用过多网络带宽，选择“最小化带宽”单选按钮即可。系统默认为“正常”状态，即不进行任何优化。
- 协议。系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表框中选择 HTTP 协议，但是还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”(PULL 模式)传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”(PUSH 模式)传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

⑧ 单击“确定”按钮，关闭“订阅属性”对话框，返回“事件查看器”窗口，如图 9-37 所示，新创建的事件订阅已经显示在窗口中。

⑨ 通过事件查看器订阅的远程计算机日志，默认将显示在“Windows 日志”的“转发的事件”项目中，如图 9-38 所示。需要注意的是，由于网络传输等多方面问题，远程计算机上产生的相关事件并不能立即转发到事件收集服务器上，通常会有一定时间的延迟。



图 9-36　“订阅源的凭据”对话框

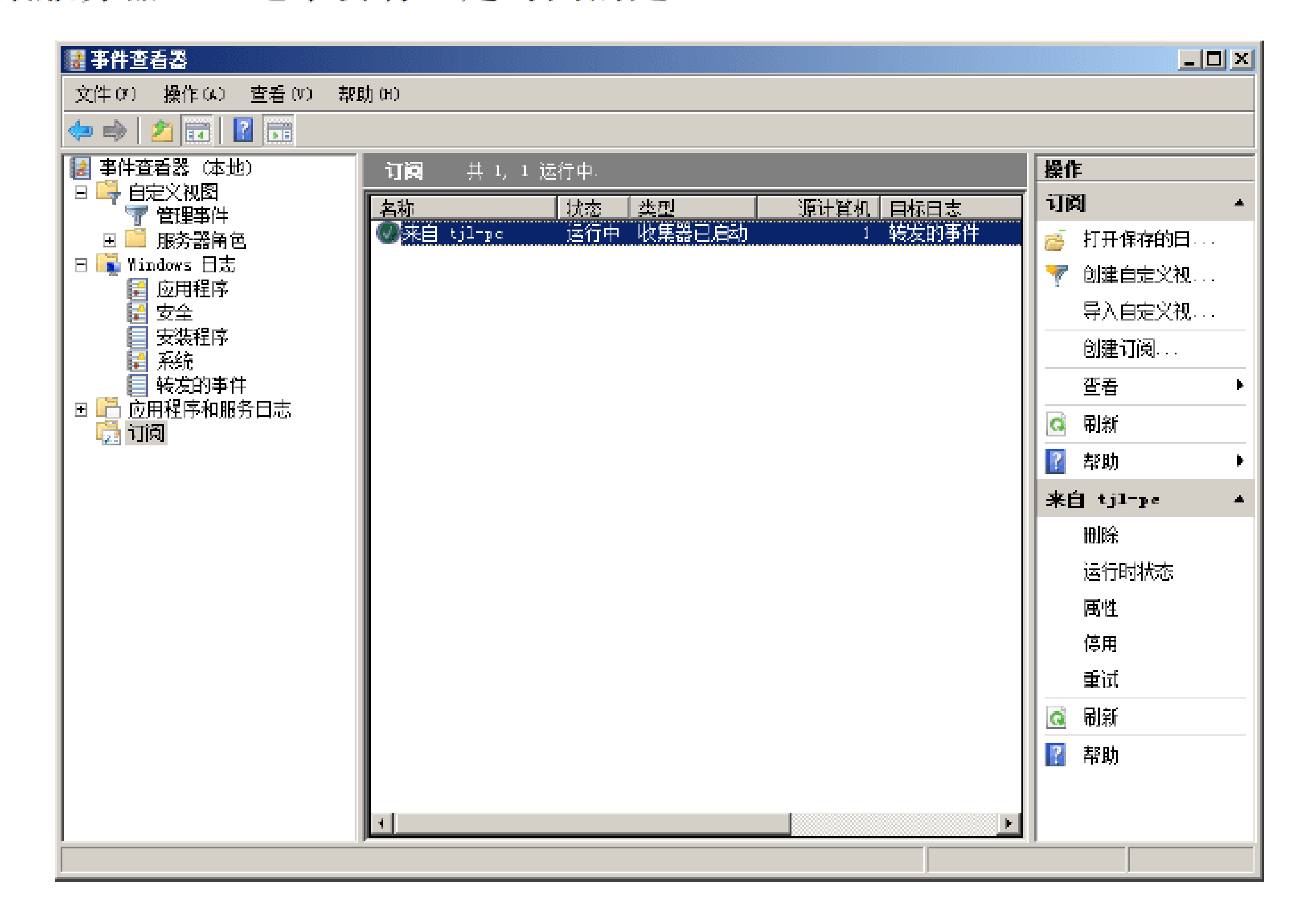



图 9-37　成功创建的订阅

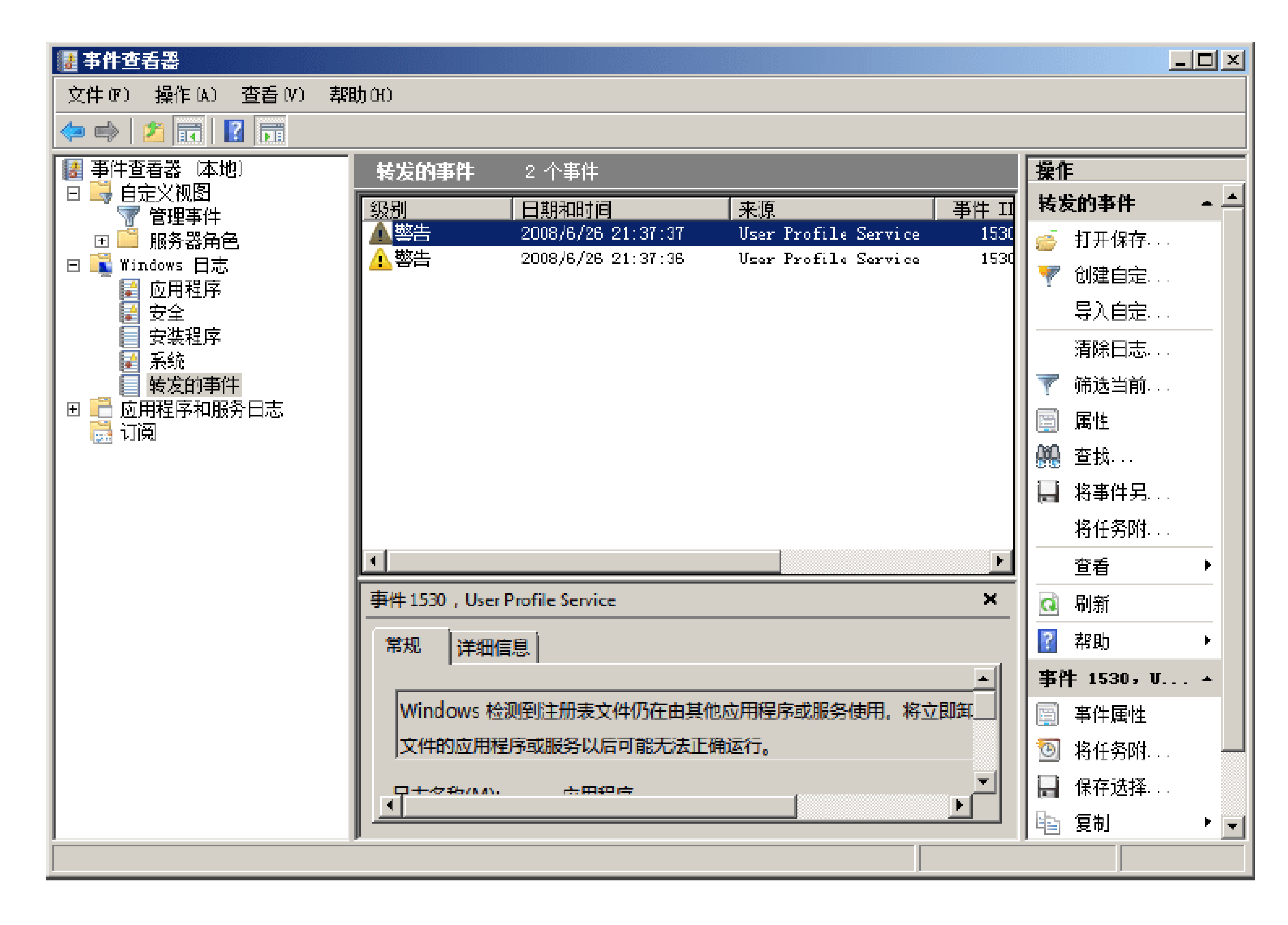


图 9-38　转发的事件

6. 分析日志和调试日志

分析日志和调试日志主要面向 IT 专业用户提供，用于分析事件产生的原因、过程等因素，对普通用户的正常应用没有太大影响。因此，默认情况下分析日志和调试日志为禁用和隐藏状态。用户可以打开“事件查看器”窗口，然后选择“查看”菜单中的“显示分析和调试日志”命令，即可在“应用程序和服务日志”列表框中看到相关的事件日志，如图 9-39 所示。

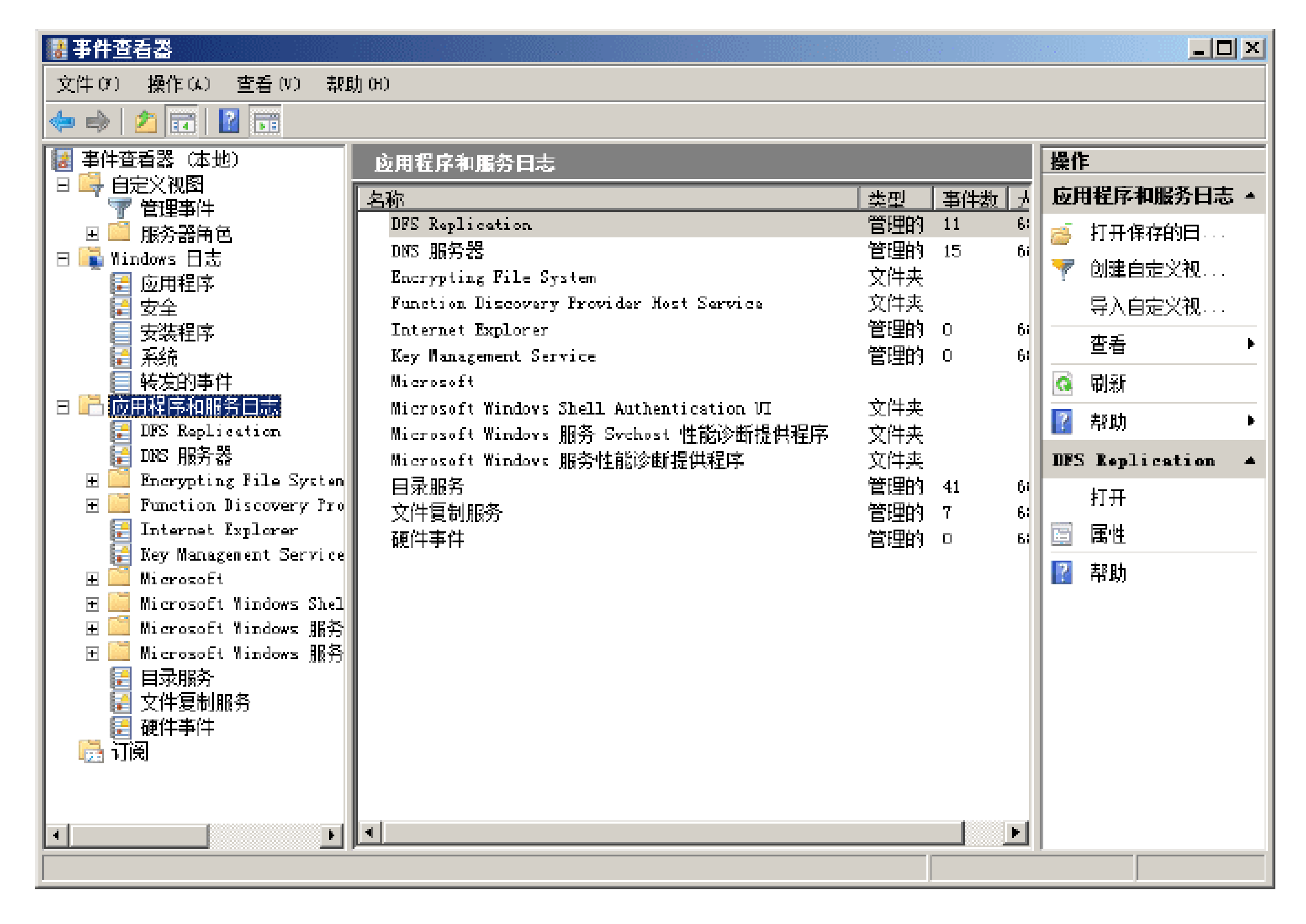


图 9-39　显示分析和调试日志

9.2　安全性日志

Windows Server 2008 系统的事件审核功能，可以帮助管理员快速检测黑客的渗透和攻击，从而防止非法用户的入侵。Windows 账户和密码是登录系统的重要凭证，通过启用对账户的审核登录功能，即可及时发现一些异常的行为和操作。据资料介绍，有 50%以上的入侵事件可以通过对账户事件的审核，发现入侵者的踪迹。

9.2.1　启用审核策略

Windows 系统可以提供 9 类事件审核策略，对于每一类都可以指明是审核成功事件、失败事件，还是两者都审核。Windows Server 2008 系统启动了大部分本地审核策略，安全性更高，管理员可以依次单击“开始”→“管理工具”→“本地安全策略”→“本地策略”→“审核策略”命令，打开 Windows 审核策略窗口，在这里即可根据需要启用或关闭安全审核策略，如图 9-40 所示。升级为域控制器的 Windows Server 2008 服务器，则需要在“组策略管理”控制台中完成。

Windows Server 2008 系统支持的事件审核策略包括如下方面。

- 审核策略更改：确定是否对用户权限分配策略、审核策略或信任策略做出更改的每一个事件进行审核。系统默认设置为“成功”，建议设置为“成功”和“失败”。
- 审核登录事件：确定是否审核用户登录到该计算机、从该计算机注销或建立与该计算机的网络连接的每一个实例。如果设定为审核“成功”，则可用来确定哪个用户成功登录到哪台计算机；如果设为审核“失败”，则可以用来检测入侵，但攻击者生成的庞大的登录失败日志，会造成拒绝服务(DoS)状态。建议保持系统设置的“成功”状态。
- 审核对象访问：确定是否审核用户访问某个对象，例如，文件、文件夹、注册表项、打印机等，它们都指定了自己的系统访问控制列表(SACL)的事件。建议设置为“失败”。
- 审核进程跟踪：确定是否审核事件的详细跟踪信息，例如，程序激活、进程退出、间接对象访问

等。如果怀疑系统被攻击，可启用该项，系统默认设置为“成功”。

图 9-40　Windows 审核策略

- 审核目录服务访问：确定是否审核用户访问那些指定有自己的系统访问控制列表(SACL)的 Active Directory 对象的事件。启用后会在域控制器的安全日志中生成大量审核项，因此只有在确实要使用所创建的信息时才应启用。系统默认设置为“成功”。
- 审核特权使用：确定是否对用户行使用户权限的每个实例进行审核，但除跳过遍历检查、调试程序、创建标记对象、替换进程级别标记、生成安全审核、备份文件和目录、还原文件和目录等权限。系统默认为“无审核”。
- 审核系统事件：用于确定当用户重新启动或关闭计算机时，或者对系统安全或安全日志有影响的事件发生时，是否予以审核。这些事件信息是非常重要的，所以建议设置为“成功”和“失败”。
- 审核账户登录事件：用于确定当用户登录到其他计算机(该计算机用于验证其他计算机中的账户)或从中注销时，是否进行审核。建议设置为“成功”和“失败”。
- 审核账户管理：用于确定是否对计算机上的每个账户管理事件，如重命名、禁用或启用用户账户，创建、修改或删除用户账户或管理事件进行审核。建议设置为“成功”和“失败”。

Windows Server 2008 本地系统审核策略的配制方法，可参考本书第 7 章中的相关介绍。审核项目应配置得当，如果审核项目过多，不仅会影响服务器的响应速度，而且还会产生大量的日志文件，加重管理员的工作负担。如果审核项目不足，则无法准确记录恶意入侵和攻击情况，降低系统安全性。管理员可以在“事件查看器”中“Windows 日志”下的“安全”目录中查看产生的安全性日志。

9.2.2　审核事件 ID

事件 ID 是 Windows 事件的基本属性之一，在 Windows 事件查看器中，管理员可以根据系统为不同类型事件定义的 ID 值，判断事件的类型和主要内容，筛选指定类型或 ID 的事件等。通过事件 ID 可以清楚地了解对服务器资源的非法访问和黑客的非法渗透。

1. 账户登录事件

表 9-3 中列出了由“审核账户登录事件”安全策略设置所生成的安全事件。

表 9-3 审核账户登录事件

类 别	事件 ID	内 容
凭据验证类别	4774	使用被映射账户进行登录
	4775	无法使用映射账户进行登录
	4776	域控制器尝试验证凭据的账户
	4777	域控制器无法验证凭据的账户
Kerberos 身份验证服务类别	4768	请求 Kerberos 身份验证票证(TGT)
	4771	Kerberos 预身份验证失败
	4772	Kerberos 身份验证票证请求失败
Kerberos 服务票证操作类别	4769	Kerberos 服务票证请求
	4770	Kerberos 服务票证已续订

2. 账户管理事件

表 9-4 中列出了由“审核账户管理”安全策略设置所生成的安全事件。

表 9-4 审核账户管理事件

类 别	事件 ID	内 容
应用程序组管理	4783	基本应用程序组已创建
	4784	基本应用程序组已更改
	4785	成员已添加到基本应用程序组
	4786	成员已从基本应用程序组删除
	4787	非成员已添加到基本应用程序组
	4788	成员被从基本应用程序组中删除
	4789	基本应用程序组已删除
	4790	已创建 LDAP 查询组
计算机账户管理	4742	计算机账户已更改
	4743	计算机账户被删除
通信组管理	4744	禁用安全的本地组已创建
	4745	禁用安全的本地组已更改
	4746	成员已被添加至禁用安全的本地组
	4747	成员已从禁用安全的本地组删除
	4748	禁用安全的本地组被删除
	4749	禁用安全的全局组已创建
	4750	禁用安全的全局组已更改
	4751	成员已添加至禁用安全的全局组
	4752	已从禁用安全的全局组删除成员

续表

类 别	事件 ID	内 容
通信组管理	4753	禁用安全的全局组已删除
	4759	禁用安全的通用组已创建
	4760	禁用安全的通用组已更改
	4761	成员已添加至禁用安全的通用组
	4762	已从禁用安全的通用组删除成员
其他账户管理事件	4739	更改域策略
	4782	账户密码哈希被访问
	4793	密码策略检查 API 调用程序
安全组管理	4727	安全启用全局组已创建
	4728	成员已添加至启用安全的全局组
	4729	已从安全启用全局组删除成员
	4730	安全启用全局组已删除
	4731	安全启用本地组已创建
	4732	成员已添加至启用安全的本地组
	4733	成员已从启用安全的本地组删除
	4734	安全启用本地组被删除
	4735	安全启用本地组已更改
	4737	安全启用全局组已更改
	4754	安全启用通用组已创建
	4755	安全启用通用组已更改
	4756	成员已添加至启用安全的通用组
	4757	成员已从启用安全的通用组删除
	4758	安全启用通用组已删除
	4764	组类型已更改
用户账户管理	4720	创建用户账户
	4722	用户账户被启用
	4723	试图更改账户的密码
	4724	试图重置账户的密码
	4725	用户账户被禁用
	4726	用户账户被删除
	4738	用户账户已更改
	4740	用户账户被锁定
	4765	SID 历史添加到账户
	4766	账户添加 SID 历史的尝试失败
	4767	已锁定用户账户
	4780	从管理员组的成员账户上设置 ACL
	4781	账户的名称已更改

续表

类　别	事件 ID	内　容
用户账户管理	4794	被试图设置目录服务还原模式
	5376	凭据管理器凭据被备份
	5377	凭据管理器凭据已从备份还原

3. 详细跟踪事件

表 9-5 中列出了由“审核进程跟踪”安全策略设置所生成的安全事件。

表 9-5　审核进程跟踪事件

类　别	事件 ID	内　容
DPAPI 活动	4692	尝试数据保护主密钥备份
	4693	尝试对数据保护主密钥进行恢复
	4694	尝试保护的审计保护数据
	4695	尝试未保护的审计保护数据
进程创建	4688	已创建一个新进程
	4696	主令牌被分配给处理
进程中止	4689	进程已退出
RPC 事件	5712	试图远程过程调用(RPC)

4. 目录服务访问事件

表 9-6 中列出了由“审核目录服务访问”安全策略设置所生成的安全事件。

表 9-6　审核目录服务访问事件

类　别	事件 ID	内　容
详细目录服务复制	4928	建立 Active Directory 副本源命名上下文
	4929	删除 Active Directory 副本源命名上下文
	4930	修改 Active Directory 副本源命名上下文
	4931	修改 Active Directory 副本目标命名上下文
	4934	复制 Active Directory 对象的属性
	4935	开始复制失败
	4936	结束复制失败
	4937	从副本延迟对象删除
目录服务访问	4662	对目录对象进行操作
目录服务更改	5136	修改目录服务对象
	5137	已创建目录服务对象
	5138	目录服务对象未删除
	5139	移动目录服务对象
	5141	删除目录服务对象

续表

类　别	事件 ID	内　容
目录服务复制	4932	Active Directory 命名上下文的副本同步已开始
	4933	Active Directory 命名上下文的副本同步已结束

5.　登录/注销事件 ID

表 9-7 中列出了“审核登录/注销事件”安全策略设置所生成的安全事件。

表 9-7　审核登录/注销事件

类　别	事件 ID	内　容
账户锁定	4625	账户无法登录
IPSec 扩展模式	4978	在扩展模式协商，IPSec 收到一个无效协商数据包。如果问题仍然存在，则可能说明网络问题或者试图修改或重播该协商
	4979	已建立 IPSec 主模式和扩展模式安全关联
	4980	已建立 IPSec 主模式和扩展模式安全关联
	4981	已建立 IPSec 主模式和扩展模式安全关联
	4982	已建立 IPSec 主模式和扩展模式安全关联
	4983	IPSec 扩展模式协商失败，相应的主模式安全关联已被删除
	4984	IPSec 扩展模式协商失败，相应的主模式安全关联已被删除
IPSec 主模式	4646	IKE 预防 DoS 攻击模式启动
	4650	已建立 IPSec 主模式安全关联，没有启用扩展模式，不使用证书验证
	4651	已建立 IPSec 主模式安全关联，没有启用扩展模式，证书用于身份验证
	4652	IPSec 主模式协商失败
	4653	IPSec 主模式协商失败
	4655	IPSec 主模式安全关联结束
	4976	在主模式协商过程中，IPSec 收到一个无效协商数据包
	5049	删除了 IPSec 安全关联
	5453	由于未启动 IKE 和 IPSec Keying 模块服务，IPSec 协商与远程计算机失败
IPSec 快速模式	4654	IPSec 快速模式协商失败
	4977	在快速模式协商过程中，IPSec 收到一个无效协商数据包
	5451	已建立 IPSec 快速模式安全关联
	5452	IPSec 快速模式安全关联结束
注销	4634	账户被注销
	4647	用户启动注销
登录	4624	已成功登录账户
	4625	账户无法登录
	4648	试图使用明确凭据登录
	4675	SID 被筛选
网络策略服务器	6272	网络策略服务器授予用户访问权限

续表

类　别	事件 ID	内　容
网络策略服务器	6273	网络策略服务器拒绝用户访问
	6274	网络策略服务器放弃用户的请求
	6275	网络策略服务器丢弃记账请求的用户
	6276	网络策略服务器隔离一个用户
	6277	网络策略服务器授权用户访问，但因为主机不符合定义策略而被阻止
	6278	主机满足网络策略服务器定义的状况策略，授予完全访问
	6279	由于重复验证失败，网络策略服务器锁定用户账户
	6280	网络策略服务器取消锁定用户账户
其他登录/注销事件	4649	检测重播攻击
	4778	重新会话已连接到窗口站
	4779	从窗口站会话被中断
	4800	锁定工作站
	4801	未锁定工作站
	4802	屏幕保护程序被调用
	4803	已关闭屏幕保护程序
	5378	请求的凭据是不允许的策略
	5632	对到无线网络进行了请求
	5633	对到有线网络进行了请求
特殊登录	4964	特殊组已分配给新登录

6. 对象访问事件

表 9-8 中列出了由“审核对象访问”安全策略设置所生成的安全事件。

表 9-8　审核对象访问事件

类　别	事件 ID	内　容
生成应用程序	4665	试图创建应用程序客户端环境
	4666	应用程序尝试的操作
	4667	删除应用程序客户端上下文
	4668	初始化应用程序
证书服务	4868	证书管理员拒绝挂起证书请求
	4869	证书服务收到重复提交的证书请求
	4870	证书服务吊销证书
	4871	证书服务收到请求来发布证书吊销列表(CRL)
	4872	证书服务发行证书吊销列表(CRL)
	4873	更改证书申请扩展
	4874	一个或多个证书申请属性更改
	4875	证书服务接收到关闭请求

续表

类　别	事件 ID	内　容
证书服务	4876	证书服务备份启动
	4877	证书服务备份完成
	4878	启动证书服务还原
	4879	证书服务还原完成
	4880	证书服务启动
	4881	证书服务停止
	4882	对于证书服务安全权限更改
	4883	证书服务检索存档密钥
	4884	证书服务证书导入其数据库
	4885	对于证书服务审核筛选器进行更改
	4886	证书服务收到证书请求
	4887	证书服务批准证书申请并颁发证书
	4888	证书服务拒绝证书申请
	4889	证书服务设置到挂起证书请求的状态
	4890	证书管理设置对于证书服务的更改
	4891	证书服务中更改一个配置项
	4892	更改属性的证书服务
	4893	证书服务存档了密钥
	4894	证书服务导入和存档密钥
	4895	证书服务 CA 证书发行到 Active Directory 域服务
	4896	已从证书数据库删除一行或多行记录
	4897	角色分离启用
	4898	证书服务加载模板
文件共享	5140	访问网络共享对象
文件系统子类别	4664	试图创建硬链接
	4985	事务的状态已更改
	5051	文件被虚拟化
筛选平台连接	5031	Windows 防火墙服务阻止应用程序接受网络上的传入连接
	5154	Windows 过滤平台具有允许应用程序或服务端口上监听传入的连接
	5155	Windows 过滤平台已阻止应用程序或服务端口上侦听传入的连接
	5156	Windows 过滤平台允许建立连接
	5157	Windows 过滤平台已阻止建立连接
	5158	Windows 过滤平台具有允许绑定到本地端口
	5159	Windows 过滤平台已阻止绑定到本地端口
筛选平台数据包过滤	5152	Windows 过滤平台阻止数据包
	5153	限制性 Windows 过滤平台筛选已阻止数据包
句柄	4656	请求句柄对象

续表

类　别	事件 ID	内　容
句柄	4658	关闭该控点来关闭对象
	4690	试图复制一个对象的句柄
其他对象访问事件	4671	应用程序试图通过 TBS 访问被阻止的序号
	4691	请求对一个对象间接访问
	4698	创建计划任务
	4699	删除计划任务
	4700	已启用计划任务
	4701	计划任务被禁用
	4702	计划任务更新
	5888	修改 COM+目录中的对象
	5889	已从 COM+目录删除对象
	5890	对象被添加到 COM+目录
注册表	4657	修改注册表值
	5039	虚拟化注册表项
Multi-use 特殊子类别	4659	对象的句柄已请求
	4660	已删除对象
	4661	请求句柄对象
	4663	试图访问对象

7. 策略更改事件

表 9-9 中列出了由“策略更改”安全策略设置所生成的安全事件。

表 9-9　策略更改事件

类　别	事件 ID	内　容
审核策略更改	4715	更改对象上的审核策略(SACL)
	4719	更改系统审核策略
	4902	创建用户审核策略表
	4904	被试图注册安全事件源
	4905	被试图注销安全事件源
	4906	CrashOnAuditFail 值已更改
	4907	更改对象上的审核设置
	4908	修改特殊组登录表
	4912	每用户审核策略更改
验证策略更改	4706	新信任创建到域
	4707	删除域信任
	4713	Kerberos 策略已更改
	4716	修改信任域信息

续表

类　别	事件 ID	内　容
验证策略更改	4717	系统安全访问已授予账户
	4718	从账户删除系统安全访问
	4864	命名空间冲突检测
	4865	添加可信任林信息项
	4866	删除可信任林信息项
	4867	修改信任信息项
授权策略更改	4704	分配用户权限
	4705	用户权限被删除
	4714	更改加密数据恢复策略
筛选平台策略更改	4709	IPSec 服务已启动
	4710	IPSec 服务被禁用
	4711	可能包含下列之一： PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本； PAStore 引擎在计算机上应用了 Active Directory 存储 IPSec 策略； PAStore 引擎在计算机上应用了本地注册表存储 IPSec 策略； PAStore 引擎无法在计算机上应用 Active Directory 存储 IPSec 策略副本； PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略失败； PAStore 引擎在计算机上应用本地注册表存储 IPSec 策略失败； PAStore 引擎无法在计算机上应用某些规则的活动 IPSec 策略； PAStore 引擎无法加载目录存储 IPSec 策略在计算机上； PAStore 引擎加载目录存储 IPSec 策略在计算机上； PAStore 引擎无法加载本地存储 IPSec 策略在计算机上； PAStore 引擎加载本地存储 IPSec 策略在计算机上； PAStore 引擎轮询以了解对活动 IPSec 策略更改，检测任何更改
	4712	IPSec 服务遇到严重错误
	5040	IPSec 设置已经更改。添加一个验证设置
	5041	IPSec 设置已经更改。验证设置了修改
	5042	IPSec 设置已经更改。删除身份验证集
	5043	IPSec 设置已经更改。添加连接安全规则
	5044	IPSec 设置已经更改。修改连接安全规则
	5045	IPSec 设置已经更改。删除连接安全规则
	5046	IPSec 设置已经更改。添加加密设置
	5047	IPSec 设置已经更改。加密设置被修改
	5048	IPSec 设置已经更改。加密设置被删除
	5440	下列标注为 Windows 筛选平台类别，在筛选引擎启动时显示
	5441	下列筛选器是 Windows 筛选平台类别，在筛选引擎启动时显示
	5442	下列提供程序是 Windows 筛选平台类别，在筛选引擎启动时显示

续表

类　别	事件 ID	内　容
筛选平台策略更改	5443	以下提供程序上下文是 Windows 筛选平台类别，在筛选引擎启动时显示
	5444	下列子层是 Windows 筛选平台类别，在筛选引擎启动时显示
	5446	Windows 过滤平台标注已更改
	5448	Windows 过滤平台提供程序已更改
	5449	Windows 过滤平台提供程序上下文已更改
	5450	Windows 过滤平台子层已更改
	5456	PAStore 引擎在计算机上应用了 Active Directory 存储 IPSec 策略
	5457	PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略失败
	5458	PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本
	5459	PAStore 引擎无法在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本
	5460	PAStore 引擎在计算机上应用了本地注册表存储的 IPSec 策略
	5461	PAStore 引擎在计算机上应用本地注册表存储的 IPSec 策略失败
	5462	PAStore 引擎无法在计算机上应用某些规则的活动 IPSec 策略。使用 IP 安全监视器管理单元来诊断问题
	5463	PAStore 引擎轮询对活动 IPSec 策略更改，检测任何更改
	5464	PAStore 引擎轮询对活动 IPSec 策略更改，检测更改，并将其应用到 IPSec 服务
	5465	PAStore 引擎接收用于强制重新加载 IPSec 策略的控件和成功处理控件
	5466	PAStore 引擎对 Active Directory IPSec 策略进行轮询，Active Directory 无法使用 Active Directory IPSec 策略的缓存副本更改。无法应用上次轮询后对 Active Directory IPSec 策略的任何更改
	5467	PAStore 引擎对 Active Directory IPSec 策略进行轮询，Active Directory 可以获得所有策略更改。Active Directory IPSec 策略的缓存副本不再被使用
	5468	PAStore 引擎通过轮询了解 Active Directory IPSec 策略更改，确定 Active Directory 可被访问，找到对应策略，并应用这些更改。Active Directory IPSec 策略的缓存副本不再被使用
	5471	PAStore 引擎加载本地存储 IPSec 策略在计算机上
	5472	PAStore 引擎无法加载本地存储 IPSec 策略在计算机上
	5473	PAStore 引擎加载目录存储 IPSec 策略在计算机上
	5474	PAStore 引擎无法加载目录存储 IPSec 策略在计算机上
	5477	PAStore 引擎无法添加快速模式筛选器
MPSSVC 规则 – 级别策略更改	4944	Windows 防火墙启动时下列策略处于活动
	4945	Windows 防火墙启动时被列出规则
	4946	Windows 防火墙例外列表已被进行更改，添加规则
	4947	Windows 防火墙例外列表已被进行更改，修改规则
	4948	Windows 防火墙例外列表已被进行更改，删除规则
	4949	Windows 防火墙设置已还原到默认值
	4950	Windows 防火墙设置已经更改

续表

类　别	事件 ID	内　容
MPSSVC 规则 – 级别策略更改	4951	规则已忽略因为通过 Windows 防火墙无法识别其主版本号
	4952	由于通过 Windows 防火墙无法识别其次要版本号部分规则已被忽略，将强制规则的其他部分
	4953	因为无法解析规则，已忽略通过 Windows 防火墙
	4954	Windows 防火墙组策略设置已更改，已应用新设置
	4956	Windows 防火墙已更改活动配置文件
	4957	Windows 防火墙未应用以下规则
	4958	由于规则引用此计算机上没有配置项目，导致 Windows 防火墙采用以下规则
其他策略更改事件	4909	更改用于 TBS 本地策略设置
	4910	更改组策略设置 TBS
	5063	试图提供加密操作
	5064	试图加密上下文操作
	5065	试图加密上下文修改
	5066	试图加密函数操作
	5067	试图加密函数修改
	5068	试图为加密函数提供操作
	5069	试图加密函数属性
	5070	试图加密函数属性修改
	5447	Windows 过滤平台筛选已被更改
	6144	成功应用了组策略对象中安全策略
	6145	处理组策略对象中的安全策略时出错
Multi-use 特殊子类别	4670	更改对象上的权限

8. 特权使用事件

表 9-10 中列出了由“审核特权使用”安全策略设置所生成的安全事件。

表 9-10　审核特权使用事件

类　别	事件 ID	内　容
敏感特权使用/非敏感特权使用	4672	特殊权限赋予新登录
	4673	特权服务调用
	4674	试图在特权对象操作

9.　审核系统事件

表 9-11 中列出了由“审核系统事件”安全策略设置所生成的系统事件。

表 9-11　审核系统事件

类　别	事件 ID	内　容
IPSec 驱动程序	4960	IPSec 丢弃传入数据包完整性检查失败。如果问题仍然存在，则可能表明网络问题或该数据包被修改传输到此计算机中。验证从远程计算机发送数据包是否与由此计算机接收相同。此错误也可能表明与其他 IPSec 实现互操作性问题
	4961	IPSec 丢弃传入数据包重播检查失败。如果问题仍然存在，则可能表明对本机的重播攻击
	4962	IPSec 丢弃传入的数据包重播检查失败消息
	4963	IPSec 丢弃应该已被保护的入站明文数据包。这通常是由于到远程计算机更改其 IPSec 策略没有通知此计算机，也可能是欺骗攻击尝试
	4965	IPSec 从远程计算机与一个正确安全参数索引(SPI)收到一个数据包。这通常由数据包被破坏的硬件故障导致的。如果持续，这些错误验证从远程计算机发送数据包是否与由此计算机接收相同。此错误也可能表明与其他 IPSec 实现互操作性问题。这时，如果连接性是畅通的，这些事件可被忽略
	5478	IPSec 服务成功启动
	5479	IPSec 服务已成功关闭。关闭对 IPSec 服务可使计算机受到更危险的网络攻击或者将计算机暴露给潜在安全风险
	5480	IPSec 服务无法获取完整的计算机上网络接口列表。这会带来潜在安全风险，因为某些网络接口的可能无法获得通过应用 IPSec 筛选器提供保护。使用 IP 安全监视器管理单元来诊断问题
	5483	IPSec 服务无法初始化 RPC 服务器。IPSec 服务无法启动
	5484	IPSec 服务遇到一个关键性失败，已关闭。关闭 IPSec 服务可能使计算机更危险的网络攻击或者将计算机暴露给潜在安全风险
	5485	IPSec 服务无法处理网络接口的即插即用事件。某些 IPSec 筛选器会因为某些网络接口的可能无法获得通过应用 IPSec 筛选器提供保护，带来潜在安全风险。 使用 IP 安全监视器管理单元来诊断问题
其他系统事件	5024	Windows 防火墙服务成功启动
	5025	Windows 防火墙服务已停止
	5027	Windows 防火墙服务无法从本地存储器检索安全策略。服务将继续强制当前策略
	5028	Windows 防火墙服务无法分析新安全策略。服务将继续实施当前策略
	5029	Windows 防火墙服务无法初始化驱动程序。服务将继续强制实施当前策略
	5030	Windows 防火墙服务无法启动
	5032	Windows 防火墙无法通知用户它阻止应用程序接受网络上传入的连接
	5033	Windows 防火墙驱动程序成功启动
	5034	Windows 防火墙驱动程序已停止
	5035	Windows 防火墙驱动程序无法启动
	5037	Windows 防火墙驱动程序检测到关键运行错误。终止
	5058	密钥文件操作
	5059	密钥迁移操作
安全状态更改	4608	正在启动 Windows
	4609	关闭 Windows

续表

类　别	事件 ID	内　容
安全状态更改	4616	更改系统时间
	4621	管理员从审核失败状态恢复系统。非管理员用户将允许进行登录。某些审核活动可能没有记录
安全系统扩展	4610	加载通过本地安全机构验证包
	4611	可信登录进程已在本地安全机构注册
	4614	通知包被加载到安全账户管理器
	4622	通过本地安全机构到加载安全程序包
	4697	系统中已安装服务
系统完整性	4612	分配给的审核消息队列的内部资源已被用尽，导致某些审核丢失
	4615	无效使用 LPC 端口
	4618	监视的安全事件模式出现图案发生
	4816	RPC 检测到解密传入的消息时的完整性冲突
	5038	代码完整性确定文件的哈希值无效。文件可能是因受到未经授权修改而损坏，或无效哈希运算错误
	5056	执行自检加密
	5057	加密基元操作失败
	5060	验证操作失败
	5061	加密操作
	5062	执行内核模式加密自检

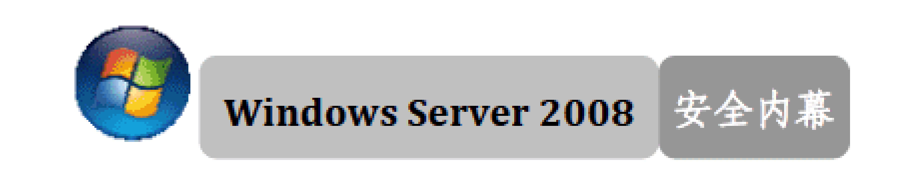
9.2.3　日志分析

在基于 NTFS 格式的操作系统中使用审核策略，虽然不能对用户的访问进行控制，但是通过打开审核产生的安全日志，可以了解系统在哪些方面存在安全隐患以及系统资源的使用情况，从而为追踪黑客提供可靠依据；同时还有利于采取相应的防范措施将系统的不安全因素降到最低，从而营造一个更加安全可靠的基于 NTFS 格式的操作系统平台。经常查看事件日志有助于预测和识别系统和安全问题的根源。

事件里的安全日志是系统安全审核的记录所在，应根据服务器的性能及选择的审核对象和记录产生速度定义好大小，一般建议为 1024MB，并定义处理方式为覆盖 30 天前的数据，这样日志中就可以保存 30 天的数据资料。如果选择了按需要覆盖，则系统记录满后将自动覆盖最早的数据(不建议)，如果选择了手工清除，请确保的日志大小足够大。安全日志记录满后如果不能自动处理，将禁止用户使用计算机。安全日志不能正确记录时，系统将立即关闭计算机。这些也可以在策略中修改。这里需要特别注意的是，当发现一个审核失败时，并不一定意味着是一个安全问题，在正常操作中，偶尔也会发生目录访问或特权使用失败的情况，应特殊问题特殊对待。

9.3　可靠性和性能

在 Windows Server 2008 和 Windows Vista 系统中，用全新的“可靠性和性能”监视工具代替了原来的“性能日志和警报”功能模块，主要功能仍是实时检查运行程序对计算机性能的影响，并收集日志数据



供以后分析使用。Windows 可靠性和性能监视器包含可合并进数据收集器集的性能计数器、事件跟踪数据和配置信息，是系统管理员的必备工具之一。

9.3.1 监视工具

Windows 可靠性和性能监视器包括 3 个监视工具：资源概述视图、性能监视器和可靠性监视器。

1. 资源概述视图

以管理员账户登录系统，依次单击“开始”→“管理工具”→“可靠性和性能监视器”命令，显示如图 9-41 所示的“资源概述”窗格。Windows 可靠性和性能监视器组合了以前独立工具的功能，包括性能日志和警报(PLA)、服务器性能审查程序(SPA)和系统监视器。它提供了自定义数据收集器集和事件跟踪会话的图表界面。

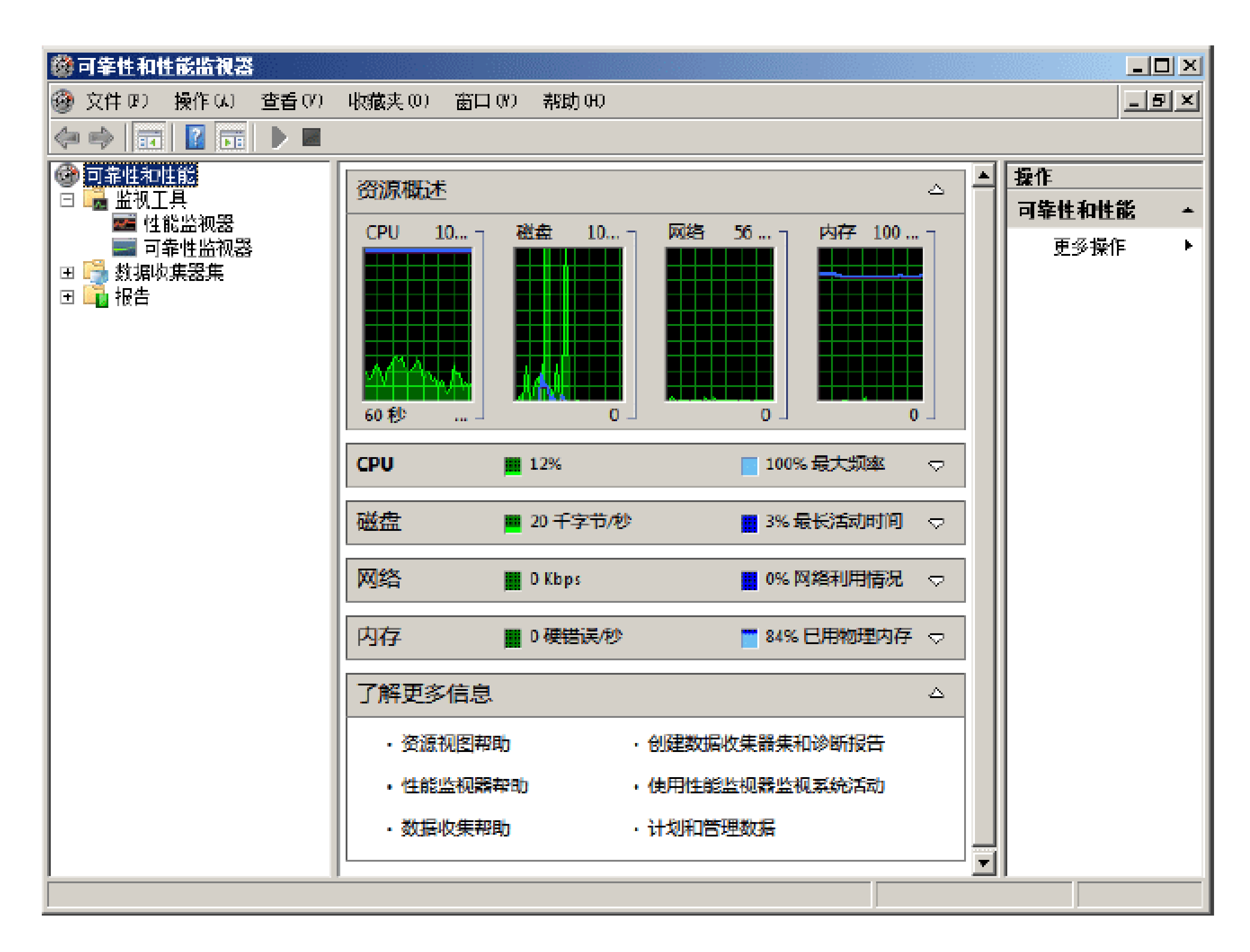


图 9-41 “资源概述”窗格

Windows 可靠性和性能监视工具的主页就是“资源概述”窗口，当用户以本地 Administrators 组成员身份登录时，可以实时监视 CPU、磁盘、网络和内存资源的使用情况和性能；并且可以通过展开 4 个资源获得详细信息。例如，展开“网络”资源，显示如图 9-42 所示的窗口，在这里用户即可查看当前系统有哪些进程正在使用网络、每个进程发送和接收的字节数、连接的远程主机 IP 地址以及本地 IP 地址等信息。

2. 性能监视器

性能监视器可以实时或查看历史数据的方式显示内置的 Windows 性能计数器。性能监视器的主要目标就是“对象”，即特定的控制服务器资源的服务或机制，例如处理器对象、内存对象、Web 对象等。每一对象的不同方面的属性称为“计数器”，因此性能监视器真正记录的是这些计数器的值，例如，处理器对象的%Processer Time 计数器、内存对象的 Pages Fault/Sec 计数器等。另外，用户也可以根据需要创建一些自定义计数器，以实现对更多功能的实时监视。

(1) 添加计数器

计数器是性能监视器工作的重要依据，Windows Server 2008 系统默认已经集成了多个计数器，用户

可以根据需要选择添加，并且随着其他应用服务的安装，还将随之创建其他计数器，可用于完成对相关事件日志的分析。如安装 IIS 组件之后就会自动添加 IIS 计数器，包括 Web 服务计数器、FTP 服务计数器等。

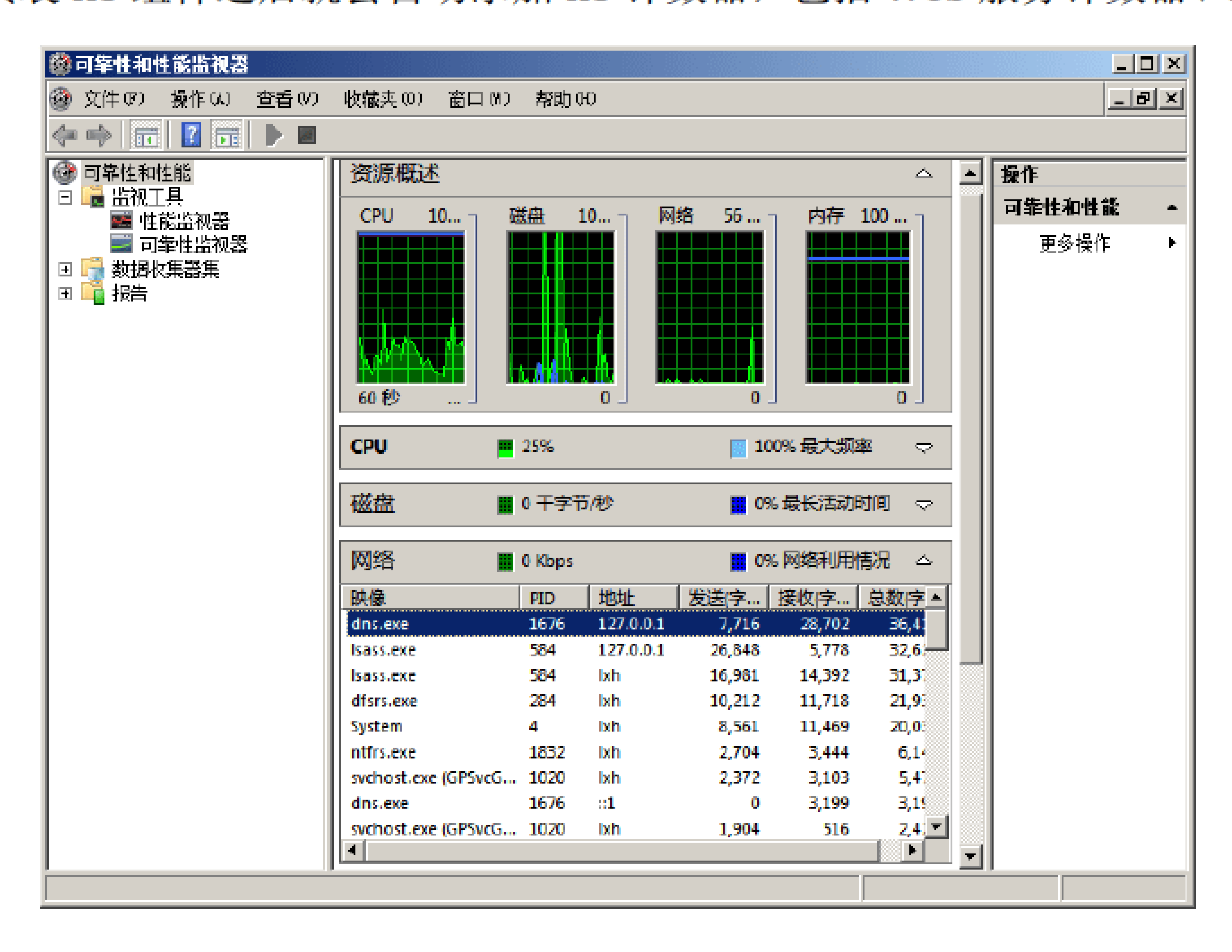


图 9-42　“网络”资源详细信息

① 在“可靠性和性能监视器”窗口中，单击“性能监视器”即可显示如图 9-43 所示的性能监视器窗格。默认情况下，系统只对本地计算机处理器运行情况进行性能监视和分析。

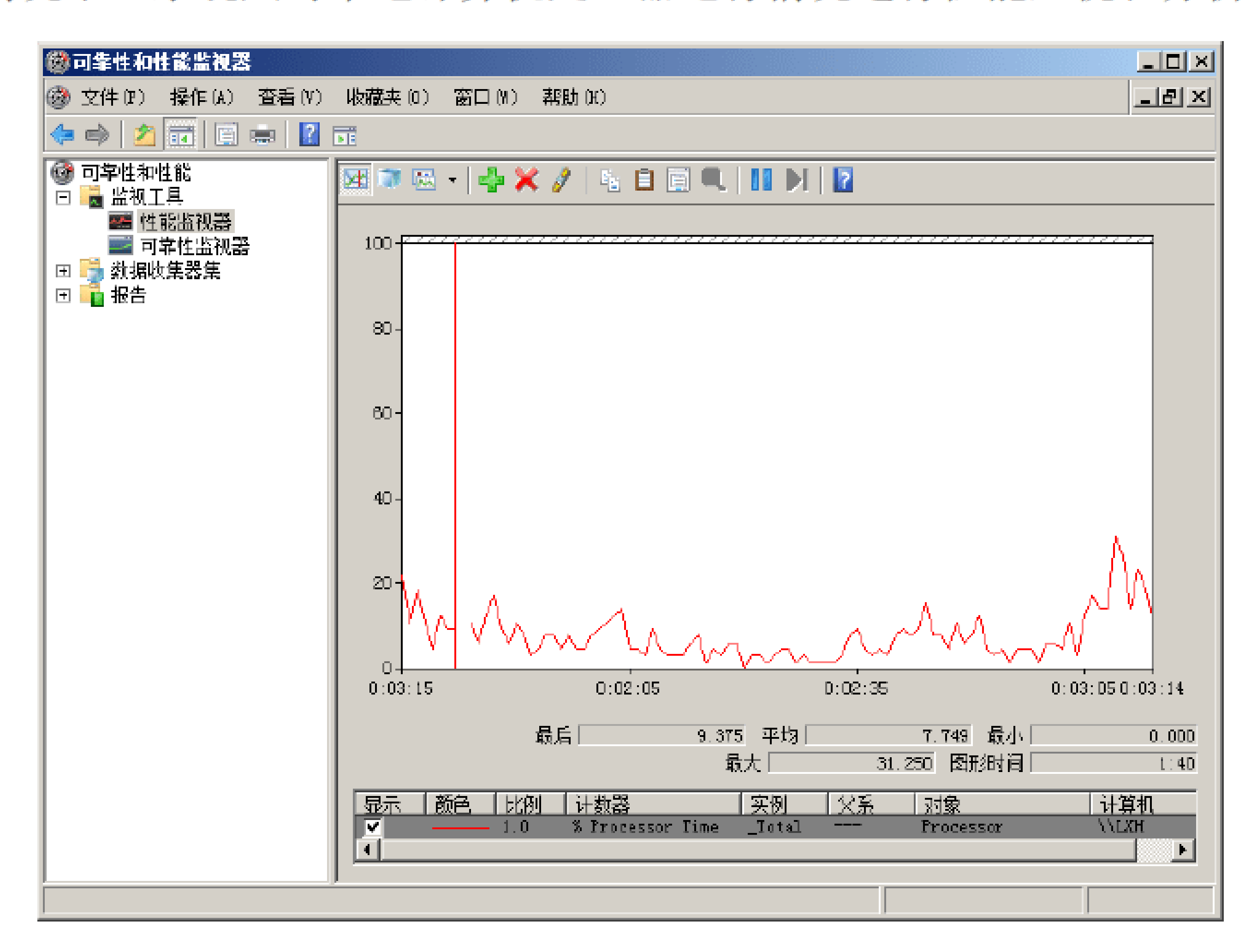


图 9-43　性能监视器窗格

② 在窗口空白处右击，并选择快捷菜单中的“添加计数器”命令，打开如图 9-44 所示的“添加计数器”对话框。在“从计算机选择计数器”列表中，选择希望应用的计数器。Windows 系统提供的监视器都是以分组方式显示的，即用户可以选择添加一组计数器，也可以选择其中的一个或者几个，然后单击“添加”按钮，即可将其添加到“添加的计数器”列表中。需要注意的是，在“性能监视器”窗口中，每个计数器的运行状态都会以不同的颜色或格式显示，如果选择计数器较多，则很难分辨，因此建议只添加自己需要的计数器。

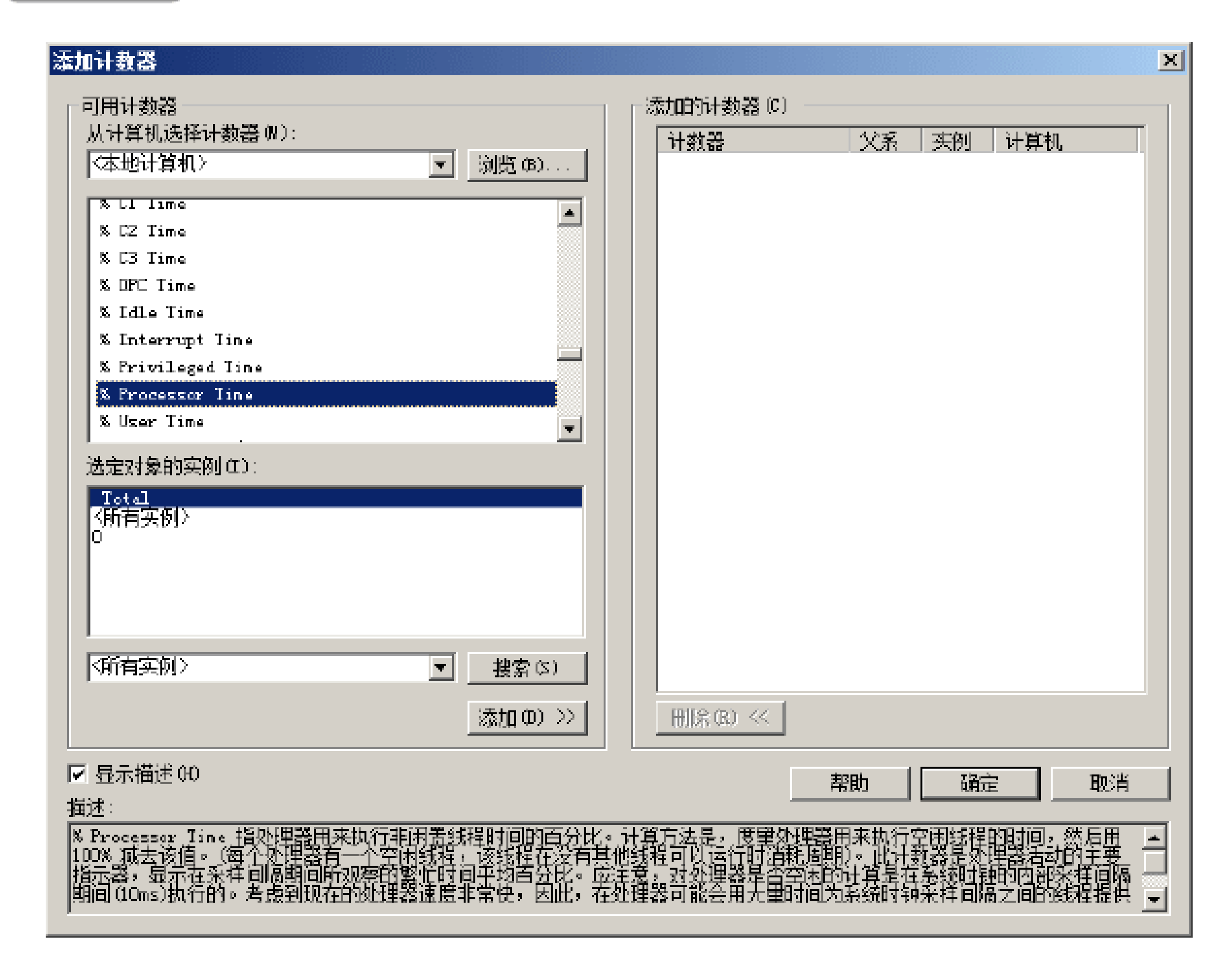


图 9-44 “添加计数器”对话框



提示：选中“显示描述”复选框，还可以查看每个计数器的详细信息。

③ 单击“确定”按钮，所选计数器即可添加到“性能监视器”窗口中，并开始工作，如图 9-45 所示。性能监视器默认以曲线形式反映监视计数器的运行情况。在工具栏中单击“更改图形类型”图标，用户还可以根据自己的需要变换信息显示方式，如直方图、报告等方式。

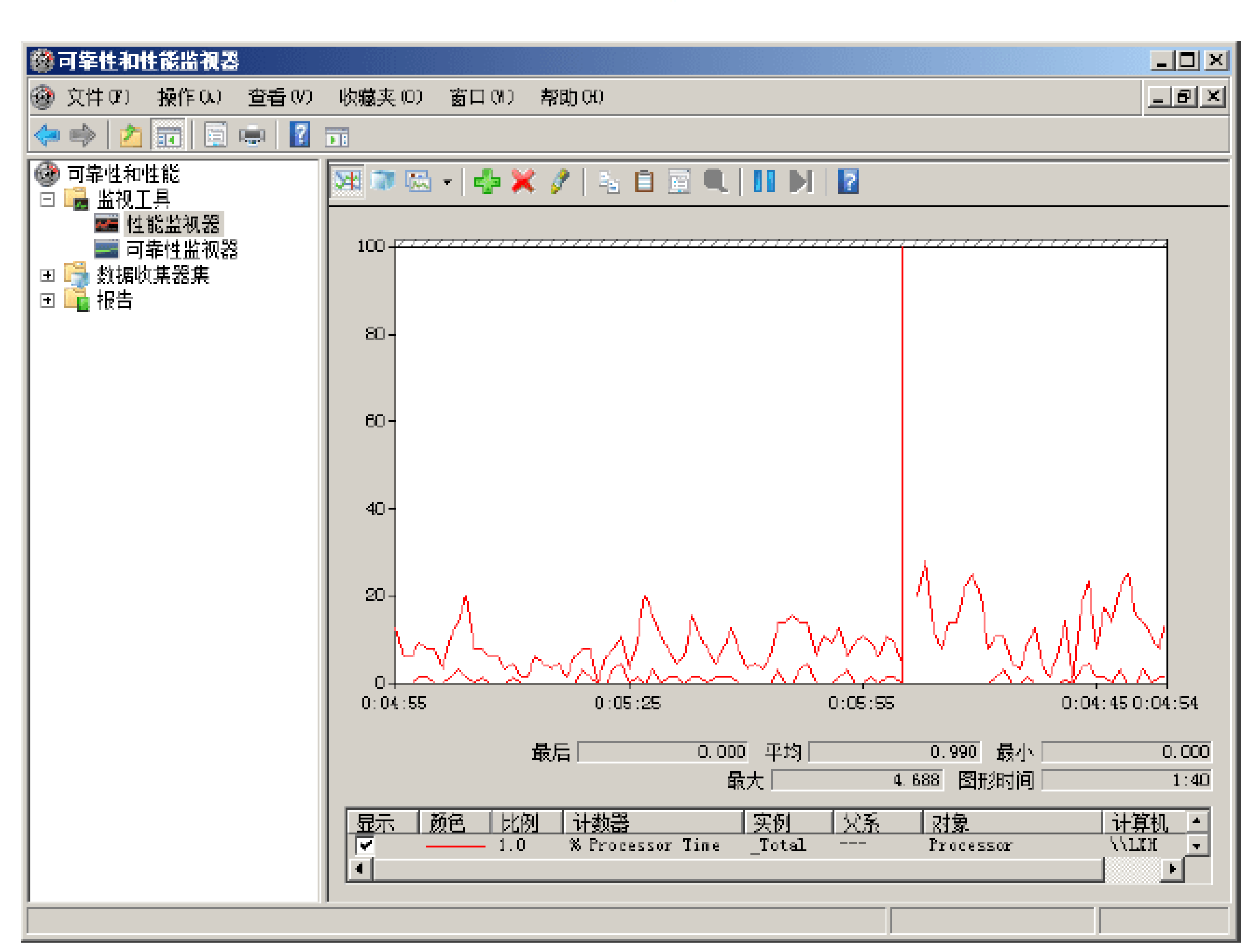


图 9-45 成功添加的计数器

注意：要执行此过程，必须是本地计算机 Administrators 组或 Performance Log Users 组的成员，或者必须被委派了适当的权限。如果计算机已加入某个域，则 Domain Admins 组的成员可能会执行该过程。

④ 在“性能监视器”窗口中右击，并选择快捷菜单中的“属性”命令，打开如图 9-46 所示的“性能监视器 属性”对话框。默认显示“数据”选项卡，即当前正在运行的所有计数器。在该选项卡中，

可以对所选计数器的显示状态进行设置，如颜色、宽度、样式等。

⑤ 单击“常规”标签切换到如图 9-47 所示的“常规”选项卡。在“显示元素”选项区域中可以设置“性能监视器”主窗口中显示的元素类型，建议保持系统默认设置，即显示所有元素，便于比对和查看。

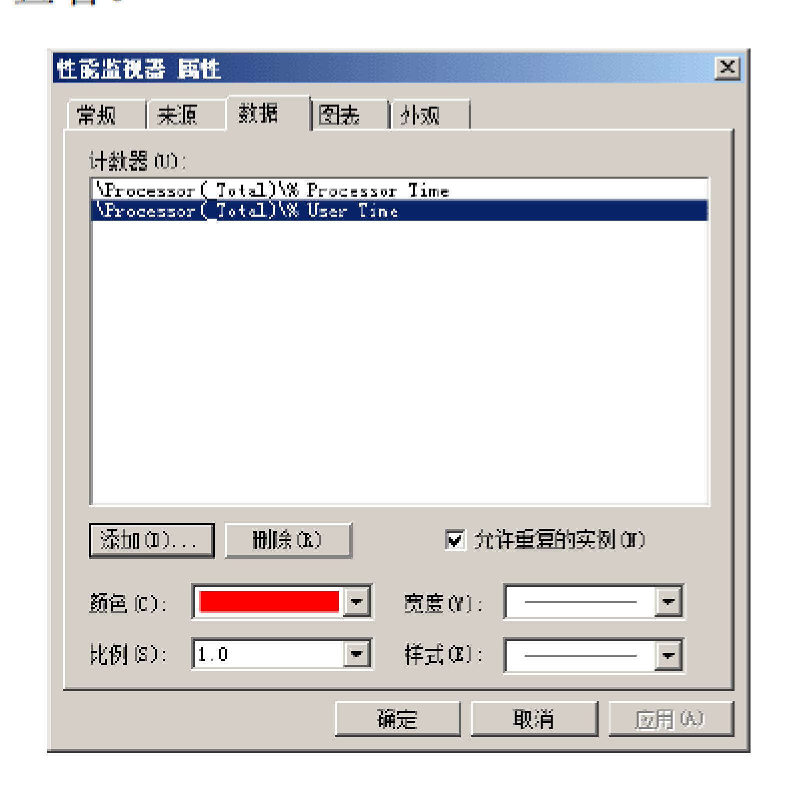


图 9-46　“性能监视器 属性”对话框

图 9-47　“常规”选项卡

⑥ 切换至“来源”选项卡，系统默认选择“当前活动”单选按钮，即以当前事件信息为数据源。选择“日志文件”单选按钮，然后单击“添加”按钮，打开“选择日志文件”对话框，选择希望查阅的事件日志即可，如图 9-48 所示。性能监视器支持 Windows 可靠性和性能监视器中产生的所有类型的日志文件。

⑦ 单击“图表”标签切换到如图 9-49 所示的“图表”选项卡。在“查看”下拉列表框中可以设置“性能监视器”默认的查看方式，系统默认的是“线条”即曲线图的查看方式，监视对象较少时可以采用这种方式；而当监视对象较多时建议采用“直方图条”；若要查看准确的数据信息则可以使用“报告”的方式。在这里还可以设置“性能监视器”显示的标题和“垂直轴”标注等，另外，为了查看更为精确的结果还可以选中“垂直格线”和“水平格线”复选框。

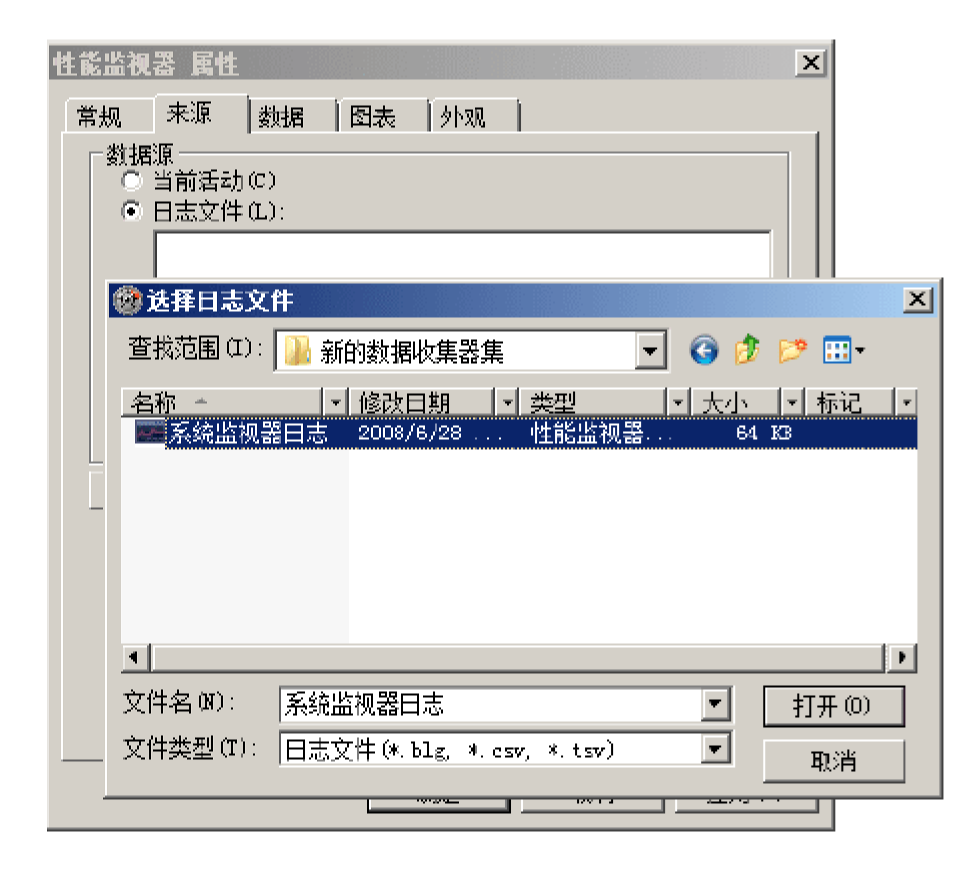


图 9-48　“来源”选项卡

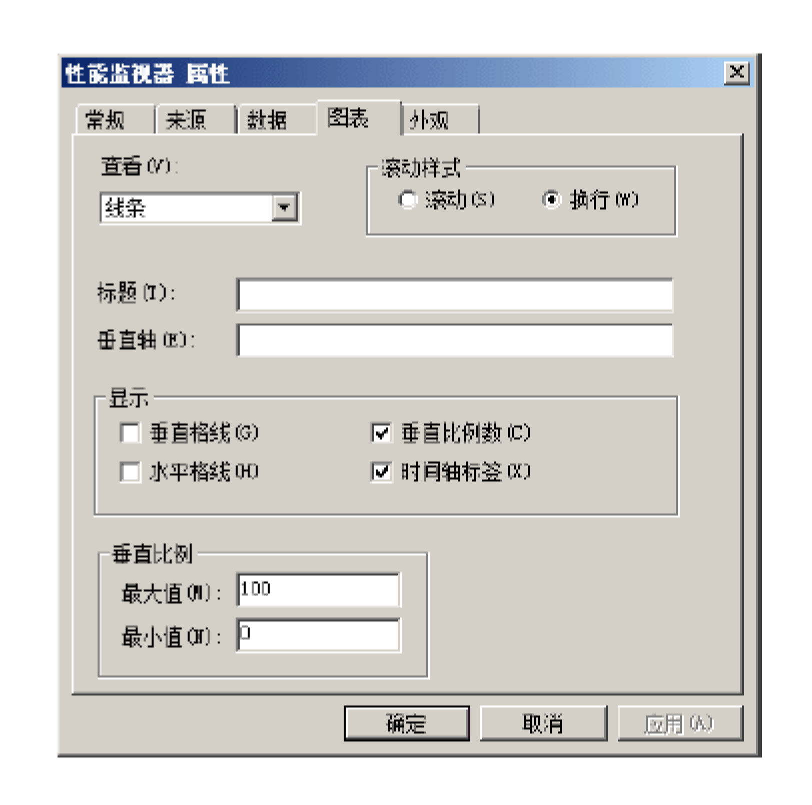


图 9-49　“图表”选项卡

(2) 删除计数器

如果添加的计算器过多，不仅严重影响服务器运行速度，而且不容易分辨。所以必要的时候要删除不

用的或非必要的计数器。删除操作非常简单，只需在性能监视器的监视对象列表中选中想要删除的计数器，然后依次单击“性能”→“删除”命令即可，或者按 Delete 键删除所选计数器。也可以在“性能监视器”窗口中右击，选择快捷菜单中的“删除所有计数器”命令，打开如图 9-50 所示的“性能监视器控制”对话框，单击“确定”按钮即可删除当前运行的所有计数器。

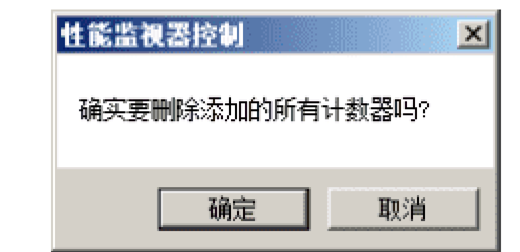


图 9-50 “性能监视器控制”对话框

(3) 常用计数器

Windows 操作系统中内置了数百个计数器，表 9-12 中列出了部分常用的计数器并做出了简要的解释。

表 9-12 常用 Windows 计数器

性能监视器对象	计 数 器	描 述
Processor	%Processor Time(所有实例)	指处理器执行非闲置线程时间的百分比。这个计数器设计成用来作为处理器活动的主要指示器。它通过在每个范例间隔中衡量处理器用于执行闲置处理线程的时间，并且用 100%减去该值得出。(每台处理器有一个闲置线程，该线程在没有其他线程可以运行时消耗周期)可将其视为范例间隔用于做有用工作的百分比。这个计数器显示在范例间隔时所看到的忙时平均值，这个值是用 100%减去该服务不活动的时间计算出来的
Processor 瓶颈	Interrupts/sec	指处理器每秒钟接收并维护的硬件中断的平均值。它不包括 DPC，DPC 将单独计算。这个值是产生中断的设备(如：系统时钟、鼠标、磁盘驱动器、数据通信线路、网络接口卡和其他附件设备)活动的间接指示器，这些设备通常在完成了一项任务或需要注意时中断处理器。正常的线程操作在中断时悬停。大多数系统时钟每隔 10ms 中断处理器一次，形成了间隔活动的后台。这个计数值显示用上两个实例中观察到的值的差除以实例间隔的持续时间所得的值
	System/Processor Queue Length(所有实例)	是指处理列队中的线程数。即使在有多个处理器的计算机上处理器时间也会有一个单列队。不像磁盘计数器，这个计数器仅计数就绪的线程，而不计数运行中的线程。如果处理器列队中总是有两个以上的线程，通常表示处理器堵塞。这个计数器仅显示上一次观察的值，而不是一个平均值
	System/Context Switches/sec	指计算机上的所有处理器全都从一个线程转换到另一个线程的综合速率。当正在运行的线程自动放弃处理器时出现上下文转换，由一个有更高优先就绪的线程占先或在用户模式和特权(内核)模式之间转换以使用执行或分系统服务。它是在计算机所有处理器上运行的所有线程的 Thread: Context Switches/sec 的总数并且用转换数量衡量。在系统和线程对象上有上下文转换计数器。这个计数值显示在上一次两个实例中观察到的值除以实例间隔的持续时间所得的值的差异
Process	Private Bytes	指这个处理不能与其他处理共享的、已分配的当前字节数
	Virtual Bytes	指处理使用的虚拟地址空间的以字节数显示的当前大小。使用虚拟地址空间不一定是指对磁盘或主内存页的相应的使用。虚拟空间是有限的，如果使用过多，可能会限制处理加载数据库的能力

续表

性能监视器对象	计 数 器	描　述
Process	Working Set	指这个处理的 Working Set 中的当前字节数。Working Set 是在处理中被线程最近触到的那个内存页集。如果计算机上的可用内存处于阈值以上，即使页不在使用中，也会留在一个处理的 Working Set 中。当可用内存降到阈值以下，将从 Working Set 中删除页。如果需要页时，它会在离开主内存返回到 Working Set 中
	Handle Count	由这个处理现在打开的句柄总数。这个数字是在这个处理中每个线程当前打开的句柄的总数
	Page Faults/sec	此值为处理器中的页面错误的计数。当进程引用特定的虚拟内存页，该页不在其在主内存的工作集当中时，将出现页面错误。如果某页位于待机列表中(因此它已经位于主内存中)，或者它正在被共享该页的其他进程所使用，则页面错误不会导致该页从磁盘中提取出
Objects	Threads	线程指在数据收集时在计算机中线程的数目。请注意这是一个即时计算而不是一个时间间隔的平均值。一个线程为一个基本的可执行实体，该实体在处理器中执行指令
Memory	Available Bytes	是计算机上可用于运行处理的有效物理内存的字节数量。是用零、空闲和备用内存表上的空间总值计算的。空闲内存指可以使用内存；零内存指为了防止以后的处理看到以前处理使用的数据而在很多页内存中充满了零的内存；备用内存是指从处理的工作集(它的物理内存)移到磁盘的，但是仍旧可以调用的内存。这个计数器只显示上一次观察到的值，它不是一个平均值
	Cache Bytes	是 System Cache Resident Bytes 的总数。System Driver Resident Bytes、System Code Resident Bytes 以及 Pool Paged Resident Bytes 计数器。该计数器只显示最后一次观察的值，它不是一个平均值
Memory 瓶颈或溢出	Pages/sec	是指为解析硬页错误从磁盘读取或写入磁盘的页数。(当处理程序请求不在本身工作集或物理内存其他地方中的代码或数据，而必须要从磁盘上检索时就会出现硬页错误)这个计数器设计成可以显示导致系统范围延缓类型错误的主要指示器。它是 Memory: Pages Input/sec 和 Memory: Pages Output/sec 的总和，是用页数计算的，以便在不用作转换的情况下就可以同其他页计数如 Memory: Page Faults/sec 作比较，这个值包括为满足错误而在文件系统缓存(通常由应用程序请求)的非缓存映射内存文件中检索的页。这个计数器显示用上两个实例中观察到的值之间的差除以实例间隔的持续时间所得的值
	Page Reads/sec	是指为解析硬页错误而读取磁盘的次数。(当处理请求的硬页错误不在工作集和物理内存其他地方中的代码或数据，而必须从磁盘上检索时就会出现硬页错误)这个计数器设计成可以显示导致系统范围延缓错误的主要指示器。这个包括要满足错误而在文件系统缓存(通常由应用程序请求)的非缓存映射内存文件中检索的页。这个计数器显示用上两个实例中观察到的值之间的差除以实例间隔的持续时间所得的值

续表

性能监视器对象	计 数 器	描 述
Memory 瓶颈或溢出	Transition Faults/sec	是指由在修改页列表、备份页表或在页错误时写入磁盘上造成的页错误数量。这些页是在没有额外磁盘活动的情况下恢复的。传输错误是在不计算每次操作时出错的页数的情况下计算错误数量。这个计数器显示用上两个实例中观察到的值之间的差除以实例间隔的持续时间所得的值
	Pool Paged Bytes	指在分页池中的字节数，分页池是系统内存(操作系统使用的物理内存)中可供对象(在不使用时可以写入磁盘的)使用的一个区域。Memory: Pool Paged Bytes 的计数方式与 Process: Pool Paged Bytes 的方式不同，因此可能不等于 Process: Pool Paged Bytes: _Total。这个计数器仅显示上一次观察的值；而不是一个平均值
	Pool Nonpaged Bytes	指在非分页池中的字节数，非分页池是指系统内存(操作系统使用的物理内存)中可供对象(指那些在不使用时不可以写入磁盘上而且只要分派过就必须保留在物理内存中的对象)使用的一个区域。Memory: Pool Nonpaged Bytes 的计数方式与 Process: Pool Nonpaged Bytes 的计数方式不同，因此可能不等于 Pool Nonpaged Bytes: _Total。这个计数器仅显示上一次观察的值，而不是一个平均值
PhysicalDisk	%Disk Time	指所选磁盘驱动器忙于为读或写入请求提供服务所用的时间的百分比。请谨慎对待% Disk Time 计数器。因为该计数器的_Total 实例不能精确反映多磁盘系统的利用率，因此使用% Idle Time 计数器也非常重要
	% Idle Time	汇报在实例间隔时磁盘闲置时间的百分比
	Disk Reads/sec	指在磁盘上读取操作的速率
	Disk Writes/sec	指在磁盘上写入操作的速率
PhysicalDisk 的瓶颈	Avg.Disk Queue Length(所有实例)	指读取和写入请求(为所选磁盘在实例间隔中列队的)的平均数
System	File Data Operations/ sec	指在计算机的所有逻辑磁盘上读取和写入操作的综合速度。这是系统的逆转率：每秒钟的文件控制操作。这个总值显示了上两个实例中观察到的值的差异除以实例间隔的时间
	Processor Queue Length	是指处理列队中的线程数。即使在有多个处理器的计算机上处理器时间也会有一个单列队。不像磁盘计数器，这个计数器仅计数就绪的线程，而不计数运行中的线程。如果处理器列队中总是有两个以上的线程通常表示处理器堵塞。这个计数器仅显示上一次观察的值，而不是一个平均值
	% Total Processor Time	系统上所有处理器都忙于执行非空闲线程的时间的平均百分比。在多处理器系统上，如果所有处理器始终处于忙碌状态，则此值为 100%；如果所有处理器的 50%处于忙碌状态，则此值为 50%；如果这些处理器中的 1/4 处于 100%忙碌状态，则此值为 25%。它可被视为有用作业占用的时间的比率。将为每个处理器分配空闲进程中的一个空闲线程，此空闲线程将消耗所有其他线程不使用的那些非生产性处理器周期

3. 可靠性监视器

可靠性监视器是 Windows 可靠性和性能监视器管理单元的一部分，可以提供系统稳定性概览和影响可靠性事件的详细信息。Windows 可靠性监视器可以通过收集的相关数据，计算出在系统的生存时间内系统稳定性图表及稳定性指数，管理员通过查看相应的稳定性历史记录，可以及时了解可能影响当前计算机安全的潜在风险，提高系统可靠性。

(1) 查看本地系统可靠性

依次单击“开始”→“管理工具”→“性能和可靠性监视器”命令，打开“可靠性和性能监视器”窗口，依次展开“监视工具”→“可靠性监视器”，显示如图 9-51 所示的“可靠性监视器”窗格。

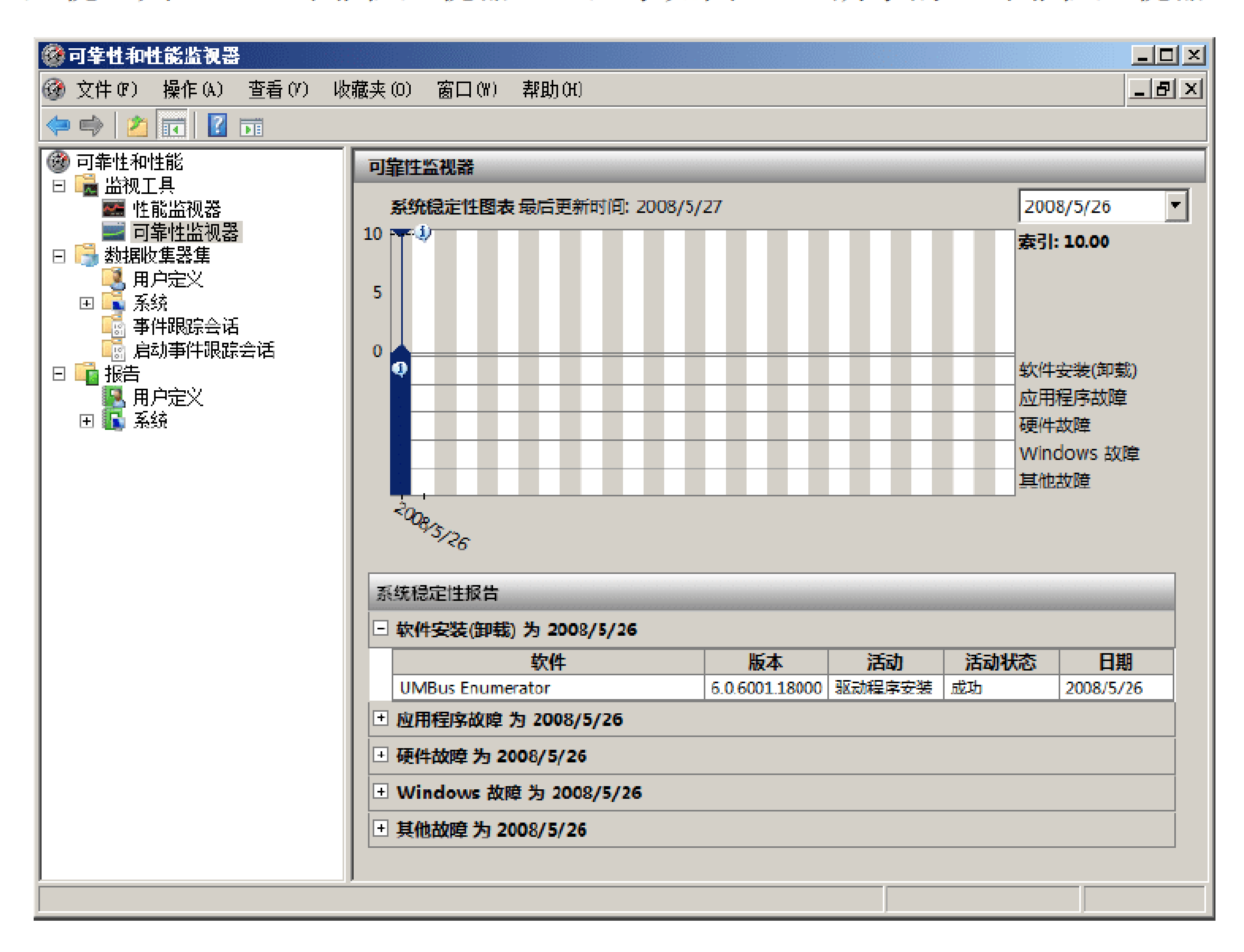


图 9-51　“可靠性监视器”窗格

“可靠性监视器”主要包括“系统稳定性图表”和“系统稳定性报告”两部分。

根据系统生存时间内收集的数据，系统稳定性图表中的每个日期都有一个显示当天系统稳定性指数分级的图形点。系统稳定性指数是一个从 1(最不稳定)到 10(最稳定)的数字，是从滚动的历史时段内所看到的特定故障的数量衍生而来的权值。在“系统稳定性图表”中选中某个图形点，即可在“系统稳定性报告”中查看对应的可靠性事件详细描述信息，如软件安装或卸载等。

(2) 启用可靠性监视器的数据收集

Windows 可靠性监视器使用由 RACAgent 计划任务提供的数据，系统安装完成后，可靠性监视器即可开始实时监控系统稳定性，并针对特定事件创建历史记录。默认情况下，RACAgent 计划任务在操作系统安装后已经自动运行。如果已禁用，则必须从 Microsoft 管理控制台中的“任务计划程序”管理单元手动启动并配置该任务。操作步骤如下。

① 以管理员账户登录系统，依次单击“开始”→“管理工具”→“任务计划程序”命令，打开“任务计划程序”窗口。在导航栏中依次展开“任务计划程序库”→Microsoft→Windows→RAC，如图 9-52 所示。

注意：默认情况下，RACAgent 计划任务是隐藏的。操作之前，首先选中 RAC，然后单击“查看”并选择下拉菜单中的“显示隐藏的任务”即可。

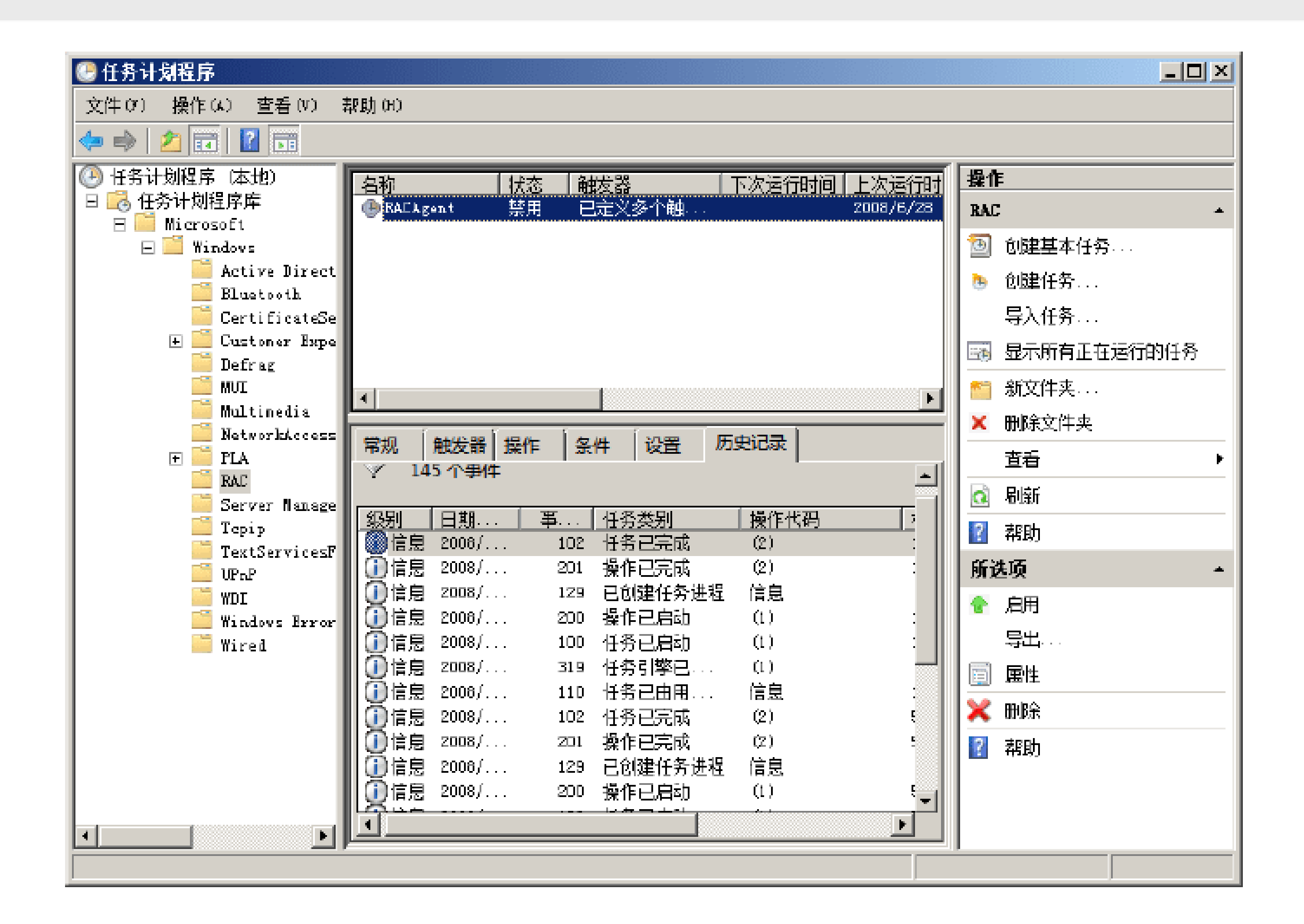


图 9-52 “任务计划程序”窗口

② 选中 RACAgent 任务，单击“操作”→“启用”命令，即可重新启用该任务。如果选择“操作”的菜单中“属性”命令，即可查看或编辑 RACAgent 任务的相关设置。默认显示如图 9-53 所示的“常规”选项卡，取消选中“隐藏”复选框即可取消 RACAgent 任务的隐藏属性。

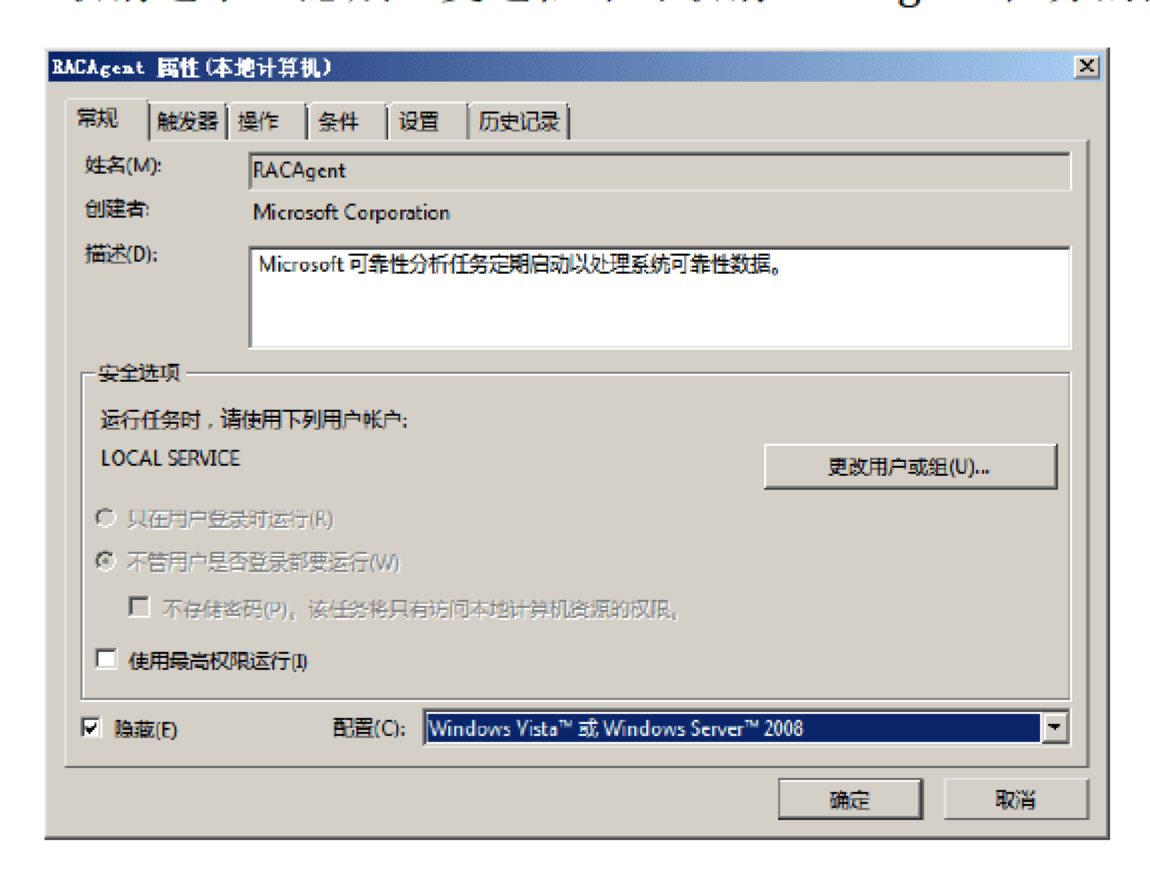


图 9-53 “常规”选项卡

③ 其他选项的配置与事件查看器中事件附加任务计划程序的配置相同，此处不复赘述。设置完成之后，单击“确定”按钮保存配置即可。

9.3.2 数据收集器集

数据收集器集是 Windows 可靠性和性能监视器中性能监视和报告的功能模块，它将多个数据收集点组

织成可用于查看或记录性能的单个组件。数据收集器集是数据收集器的集合，而数据收集器是各种计数器的集合。数据收集器收集到的数据信息将自动记录到日志中，管理员既可以在 Windows 性能监视器中查看，也可以选择通过其他非 Microsoft 应用程序查看。

1. 创建数据收集器集

Windows 数据收集器集中包括 3 种类型的数据收集器：性能计数器、事件跟踪数据、系统配置信息(注册表项值)。管理员可以根据需要通过不同的方式，创建所需类型的数据收集器集。

(1) 通过性能监视器创建数据收集器集

Windows 性能监视器不仅可以帮助管理员监控某些系统功能或组件的实时工作情况，还可以用来对数据收集器产生的历史数据进行分析和浏览，因此在“性能监视器”工具中同样可以创建收据收集器，创建完成的数据收集器集将显示在“数据收集器集”→“用户定义”目录中。

① 在“性能和可靠性监视器”窗口中，右击“性能监视器”并选择快捷菜单中的“新建”→“数据收集器集”命令，打开如图 9-54 所示的“创建新的数据收集器集”对话框。在“名称”文本框中，输入数据收集器集的名称。

② 单击“下一步”按钮，显示如图 9-55 所示的“您希望将数据保存在什么位置”界面，建议使用系统默认的保存目录，以便在“性能监视器”中可以直接查找和调用历史记录。

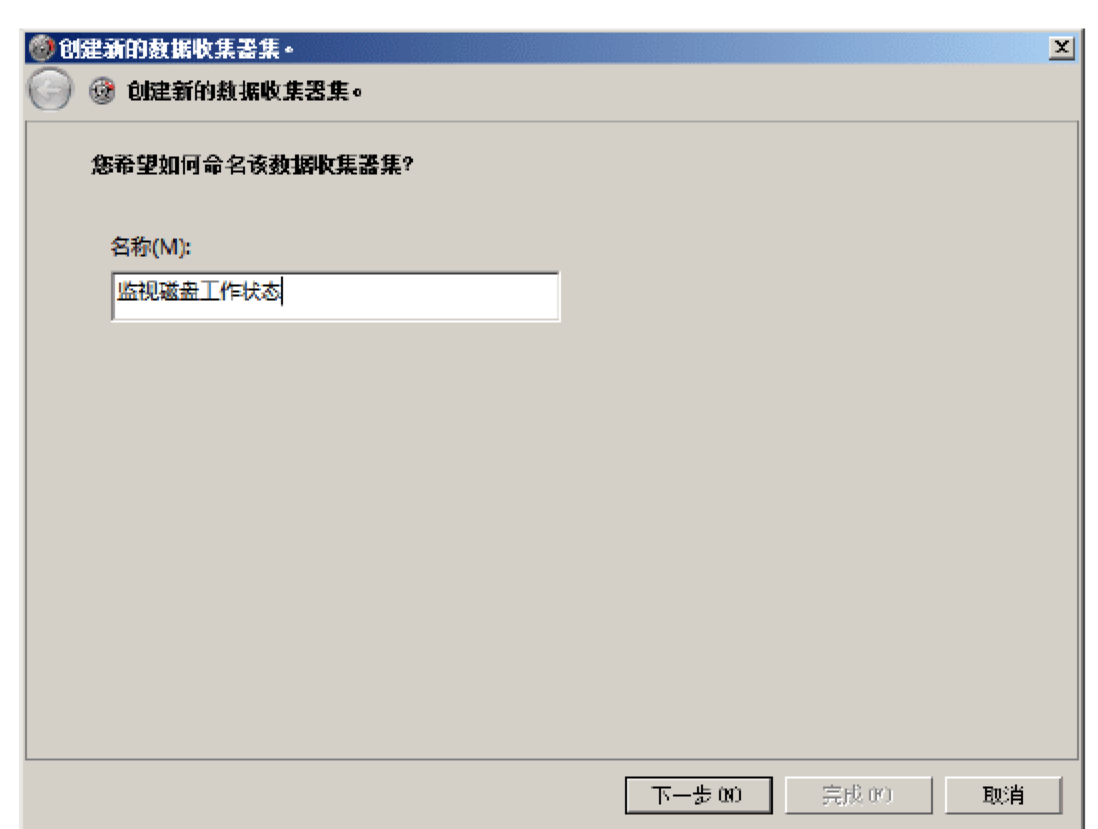


图 9-54　“创建新的数据收集器集”对话框

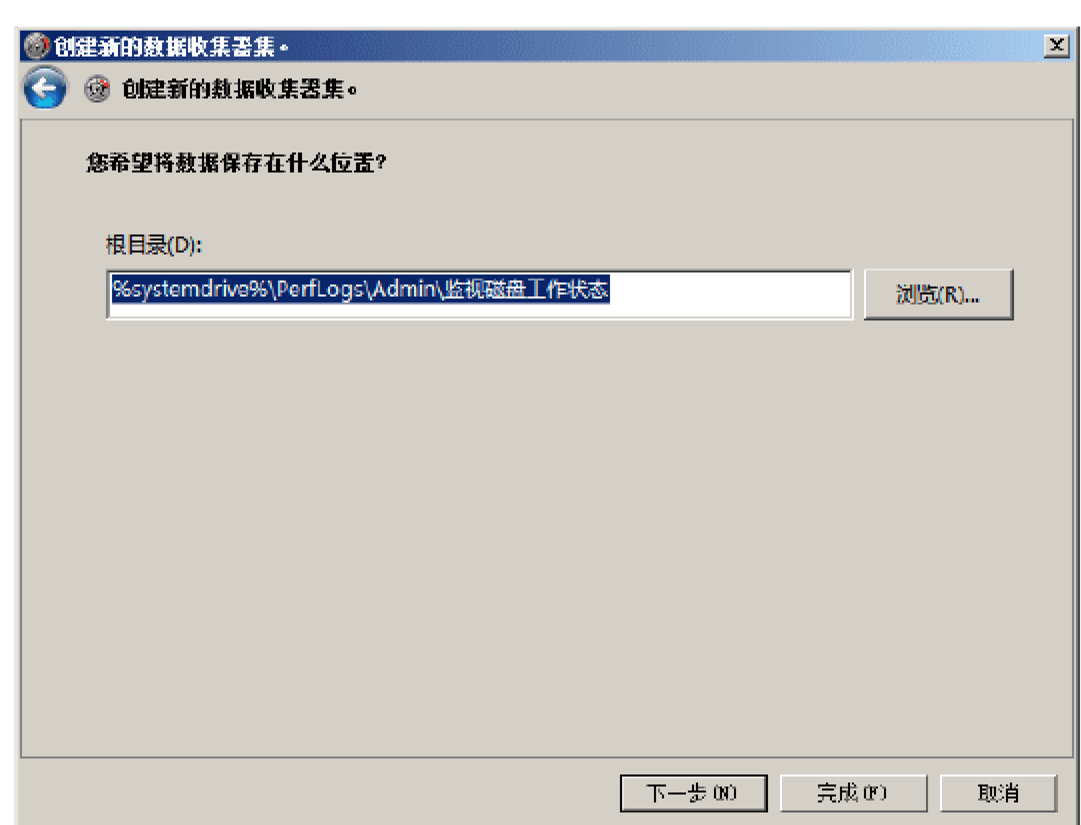


图 9-55　“您希望将数据保存在什么位置”界面

③ 单击“下一步”按钮，显示如图 9-56 所示的“是否创建数据收集器集”界面，系统默认选择“保存并关闭”单选按钮，即创建完成后并不立即启动。本例中选择“立即启动该数据收集器集”单选按钮，以便立即开始监控。



提示：单击“更改”按钮可以更改允许启动该数据收集器集的用户账户。如果当前用户账户是 Performance Log Users 组的成员，则必须将创建的数据收集器集配置为在其凭据下运行。

④ 单击“完成”按钮，关闭“创建新的数据收集器集”向导。在“可靠性和性能监视器”窗口中，展开“数据收集器集”→“用户定义”项目，即可看到创建成功的数据收集器集，如图 9-57 所示。

(2) 通过模板创建数据收集器集

Windows Vista 和 Windows Server 2008 系统中，默认已经包含一些集中于常规系统诊断信息或者收集

特定于服务器角色或应用程序的性能数据的模板。用户可以借助这些模板快速创建所需的数据收集器集。此外，还可以导入在其他计算机上创建的模板，或者将自己创建的数据收集器集保存为模板，以便下次可以直接应用。



图 9-56 “是否创建数据收集器集”界面

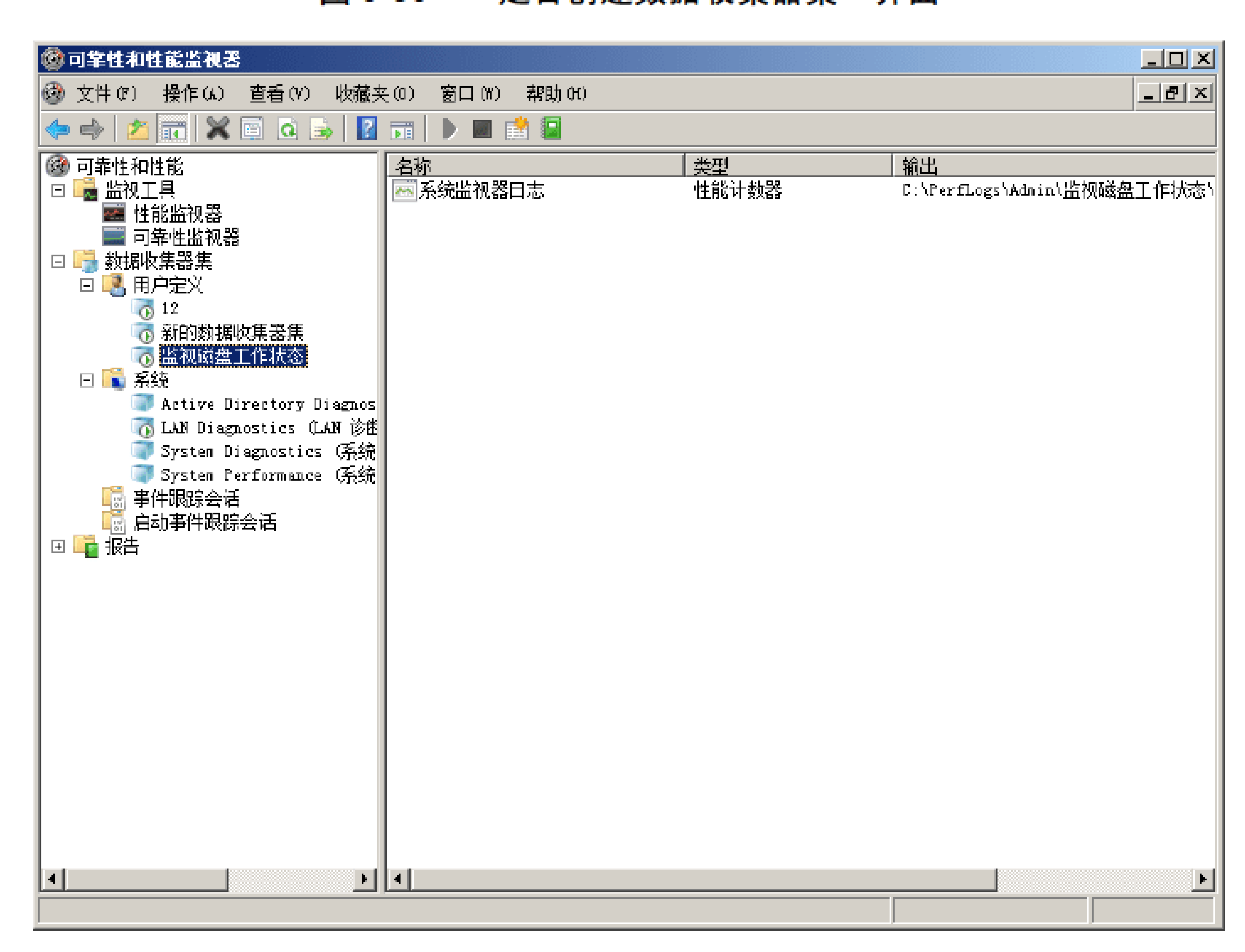
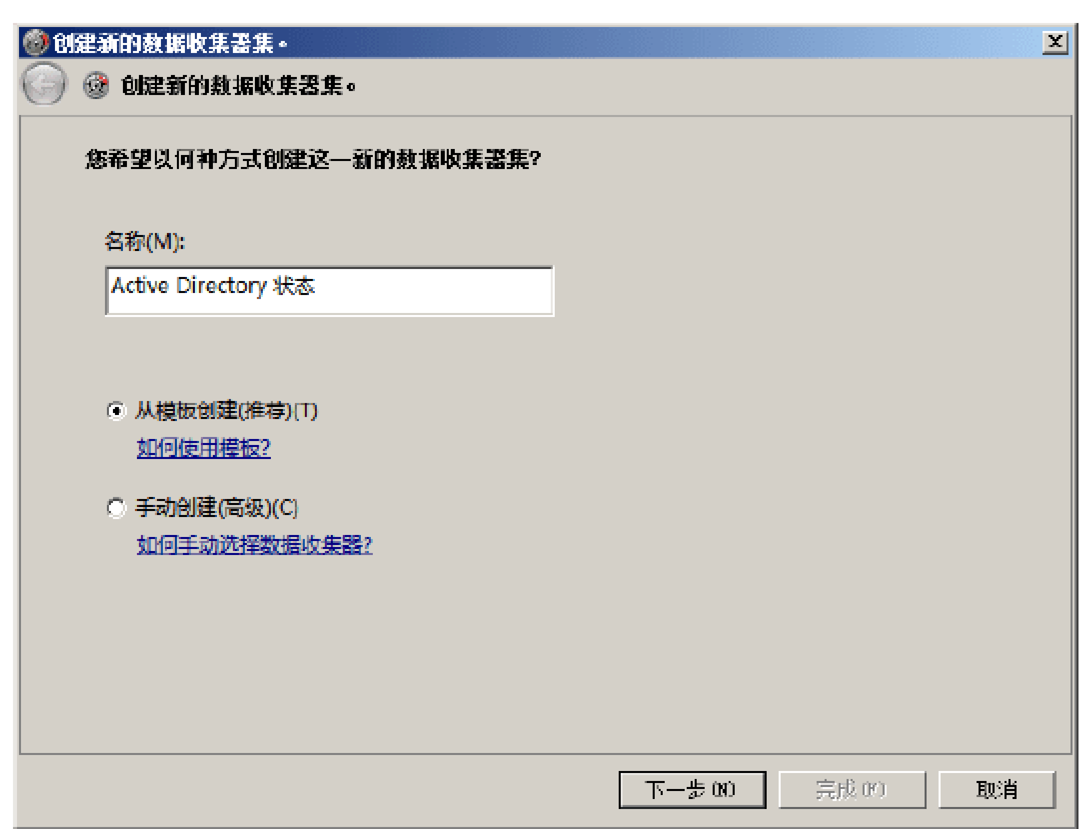


图 9-57 创建成功的数据收集器集

① 在“可靠性和性能监视器”窗口中，依次展开“可靠性和性能”→“数据收集器集”→“用户定义”，右击“用户定义”并选择快捷菜单中的“新建”→“数据收集器集”命令，启动创建新数据收集器集向导，如图 9-58 所示。在“名称”文本框中输入数据收集器集的名称，并选择“从模板创建”单选按钮。

② 单击“下一步”按钮，显示如图 9-59 所示的“您想使用哪个模板”界面。在“模板数据收集器集”列表框中选择 Active Directory Diagnostics 即可。除此之外，还可以单击“浏览”按钮添加来自本地计算机或远程计算机的模板。



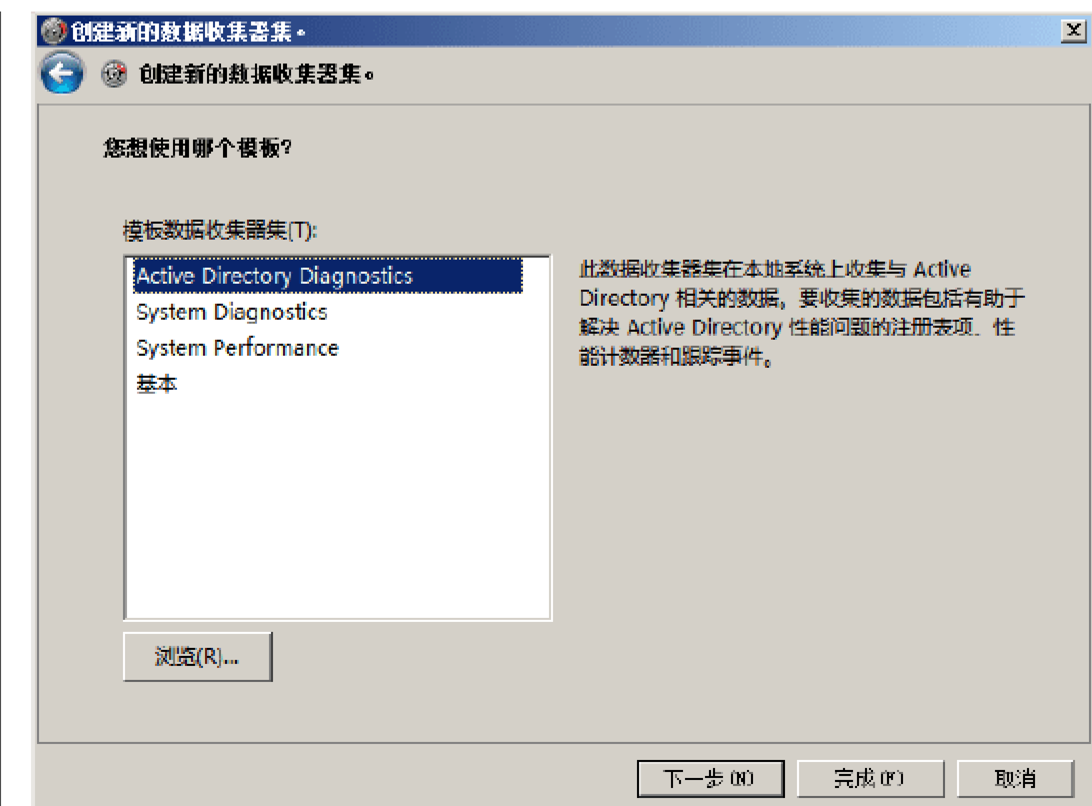


图 9-58 选择创建数据收集器集的方式　　图 9-59 “您想使用哪个模板”对话框

③ 单击“下一步”按钮，打开“你希望将数据保存在什么位置”对话框，与通过“性能监视器”创建数据收集器集相同，保持默认目录即可。单击“下一步”按钮，显示如图 9-60 所示的“是否创建数据收集器集”界面。与前面不同的是，在这里可以直接选择“打开该数据收集器集的属性”单选按钮，关闭向导后立即编辑数据收集器集属性。

④ 单击“完成”按钮，打开如图 9-61 所示的“Active Directory 状态 属性”对话框。管理员可以根据需要设置数据收集器集日志记录保存路径、文件名格式、NTFS 访问控制等。



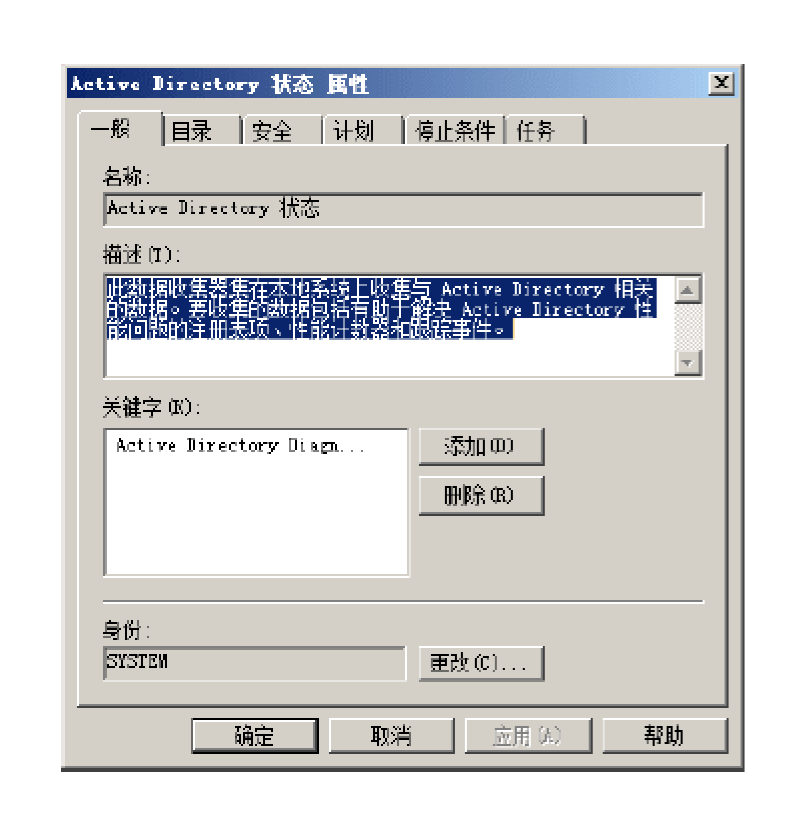


图 9-60 “是否创建数据收集器集”界面　　图 9-61 “Active Directory 状态 属性”对话框

⑤ 单击“确定”按钮保存设置并关闭对话框，此时创建的数据收集器集处于“停止”状态，右击“Active Directory 状态”并选择快捷菜单中的“开始”命令即可启动。基于系统模板创建的数据收集器集中默认已经提供了多组相关的计数器，但是管理员也可以根据需要增减，如图 9-62 所示。

(3) 手动创建数据收集器集

手动创建数据收集器集同样需要借助创建数据收集器集向导完成，与通过模板创建数据收集器集类似，不同的是管理员可以根据自己的需要定制适当的数据类型收集器。主要操作步骤如下。

① 在“可靠性和性能监视器”窗口中，依次展开“可靠性和性能”→“数据收集器集”→“用户定义”，右击“用户定义”并选择快捷菜单中的“新建”→“数据收集器集”命令，启动创建新数

据收集器集向导，如图 9-63 所示。在“名称”文本框中输入数据收集器集的名称，并选择“手动创建”单选按钮。

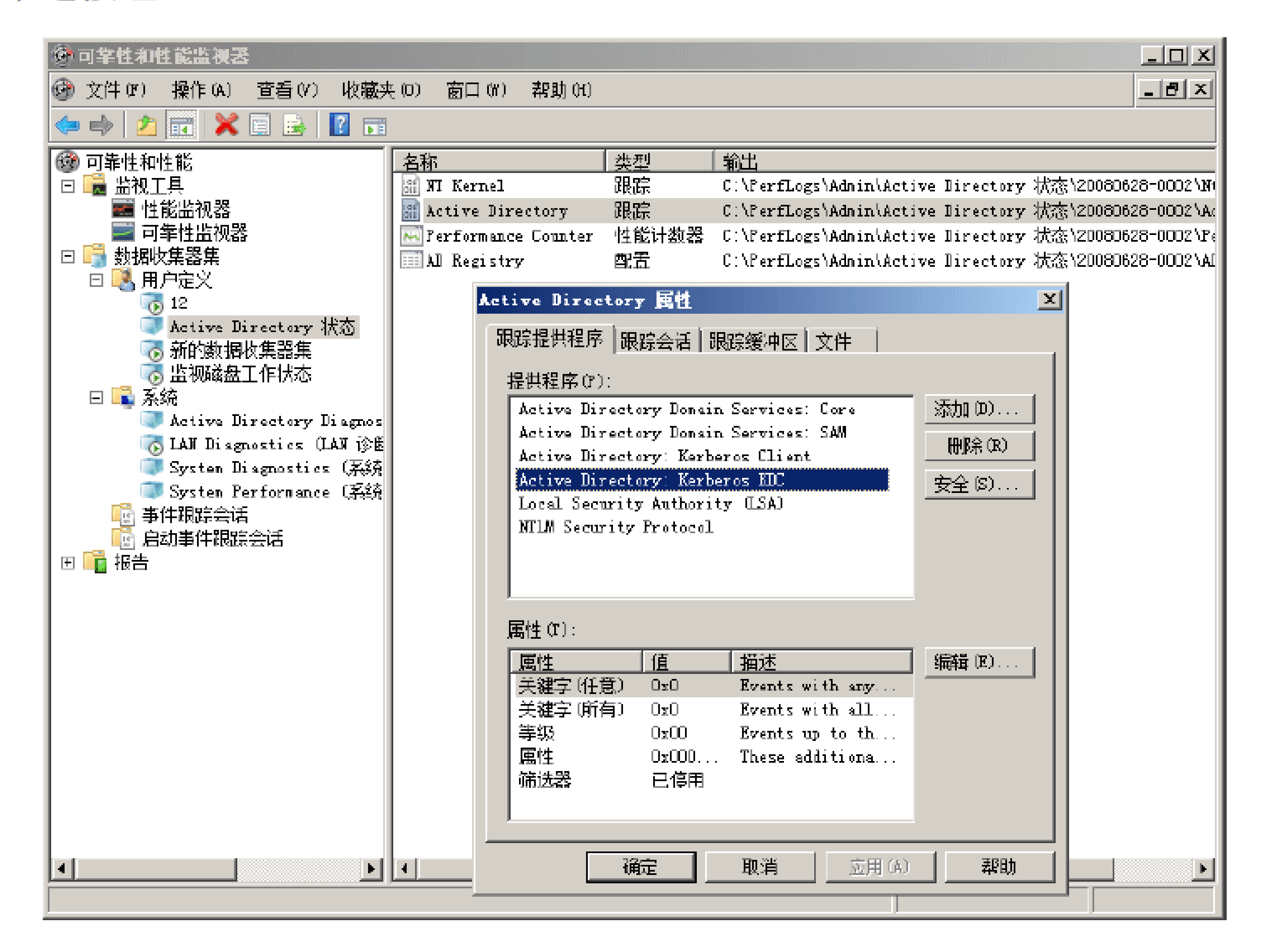


图 9-62　编辑数据收集器集中的收集器和计数器

② 单击“下一步”按钮，显示如图 9-64 所示的“您希望包括何种类型的数据”界面。选择“创建数据日志”单选按钮，并选中“事件跟踪数据”复选框。

- 性能计数器。提供有关系统性能的度量数据。
- 事件跟踪数据。提供有关活动和系统事件的信息。
- 系统配置信息。使用户可以记录注册表项的状态及对其进行的更改。

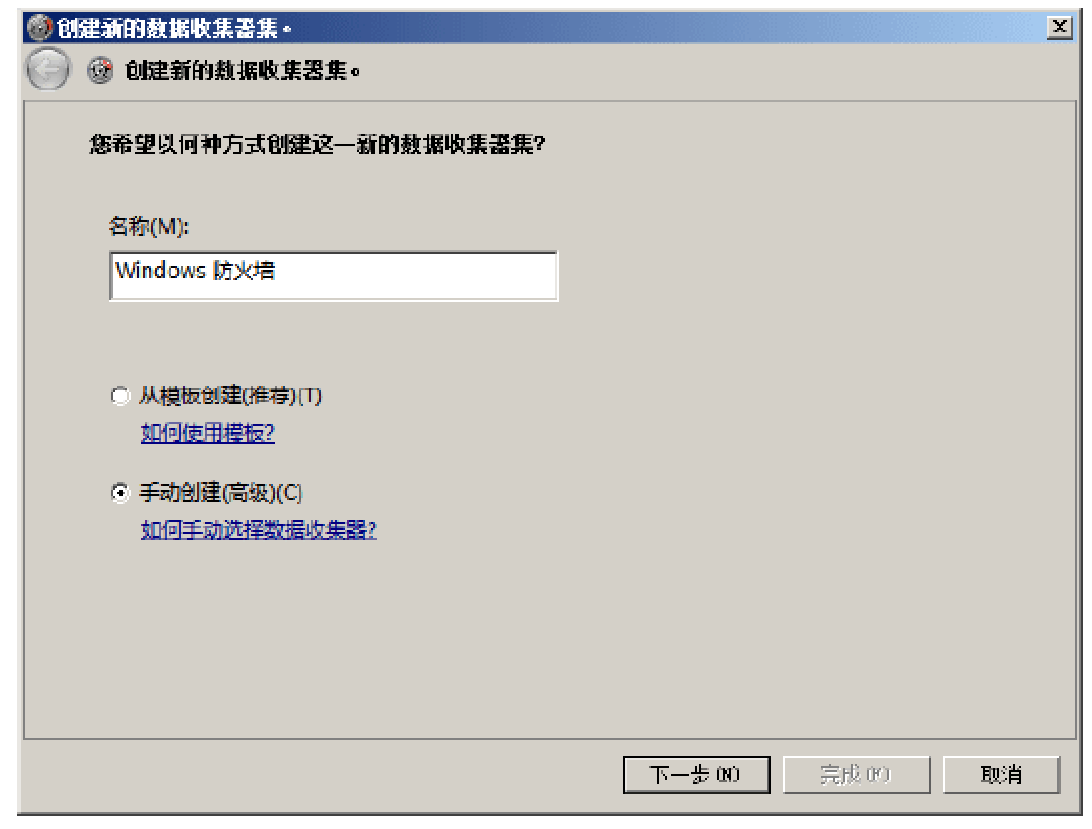


图 9-63　手动创建数据收集器集



图 9-64　“您希望包括何种类型的数据”界面



提示：选择“性能计数器警报”单选按钮，即可创建相关系统事件的警报，选择提供程序后设定相应的临界值即可。

③ 单击“下一步”按钮，打开“您希望启用哪个事件跟踪提供程序”对话框，单击“添加”按钮打开“事件跟踪提供程序”对话框，选中 Microsoft-Windows-Firewall 程序，如图 9-65 所示。

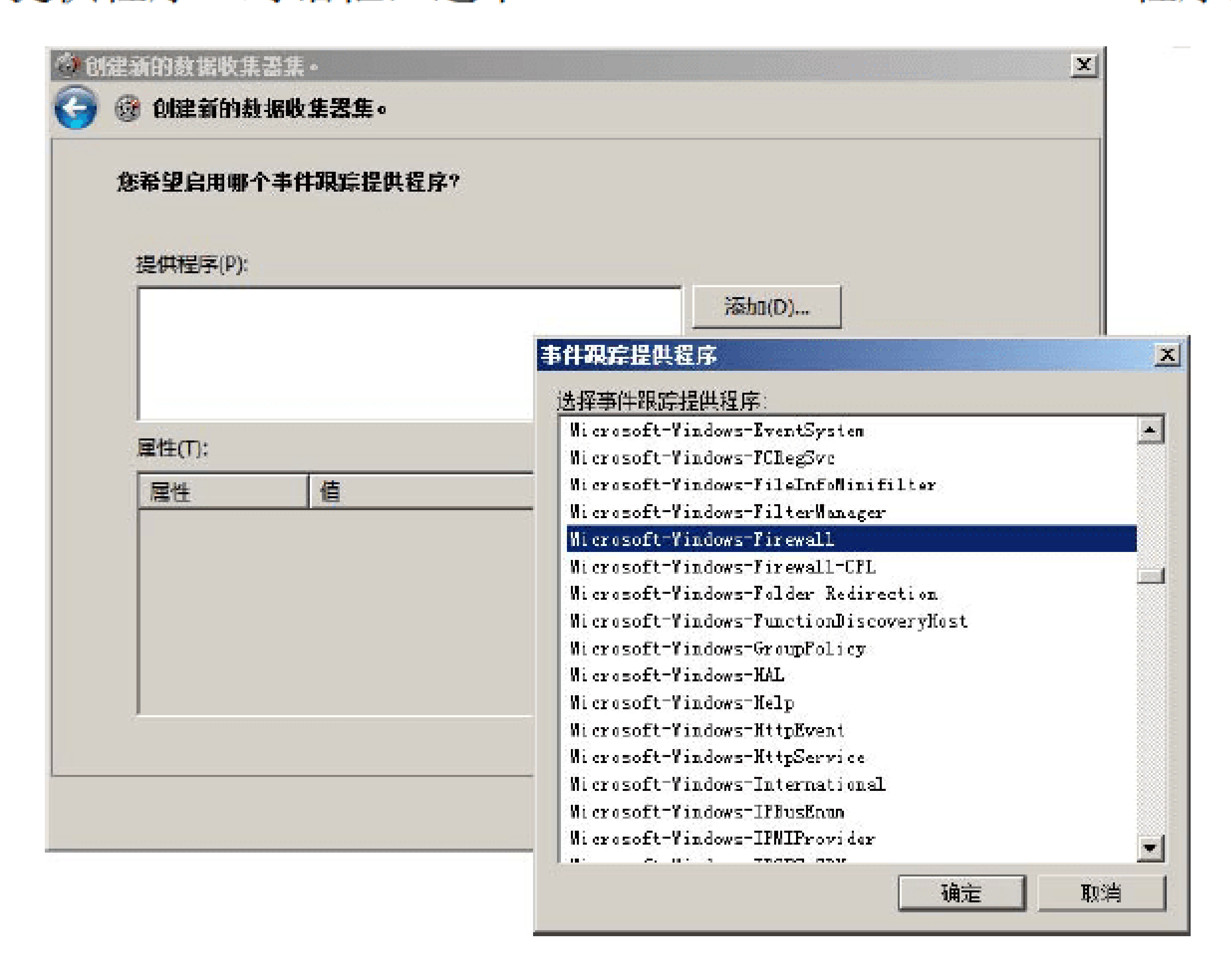


图 9-65　“事件跟踪提供程序”对话框

④ 单击“确定”按钮将所选程序添加到“提供程序”列表中，如图 9-66 所示。在“属性”列表中，选择属性后单击“编辑”按钮即可修改相应的值。

⑤ 单击“下一步”按钮，设置保存日志的目录、启动方式等信息。与通过其他方式创建数据收集器集的操作完全相同，此处不复赘述。

2. 创建数据收集器

在导航栏中，右击已创建的数据收集器集，并选择快捷菜单中的“新建”→“数据收集器”命令，打开如图 9-67 所示的“您希望创建何种类型的数据收集程序”界面，在“名称”文本框中输入数据收集器的名称，默认为“新的数据收集器”。然后选择希望创建的收集器类型，包括性能计数器数据收集程序、事件跟踪数据收集程序、配置数据收集程序和性能计数器警报 4 种。接下来的操作根据所选类型的不同，可能需要添加性能计数器、性能事件提供程序或注册表项等，只需按照向导提示逐步操作即可。

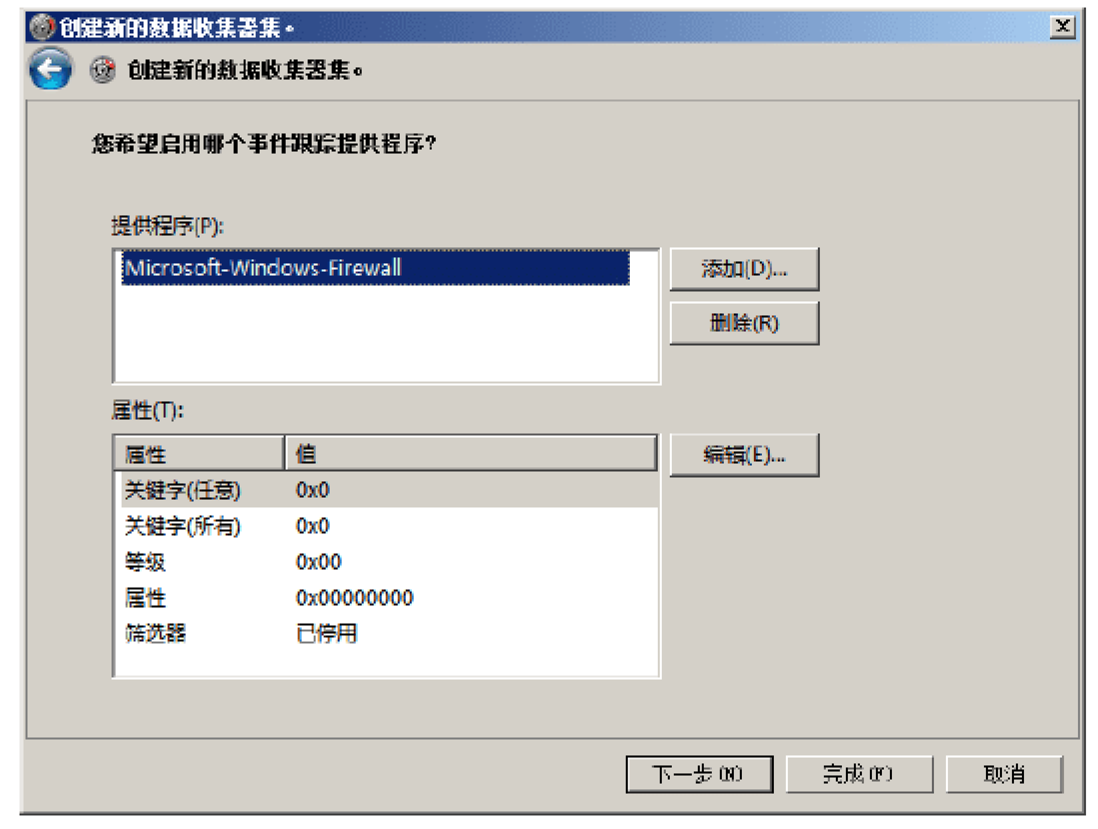


图 9-66　“您希望启用哪个事件跟踪提供程序”界面

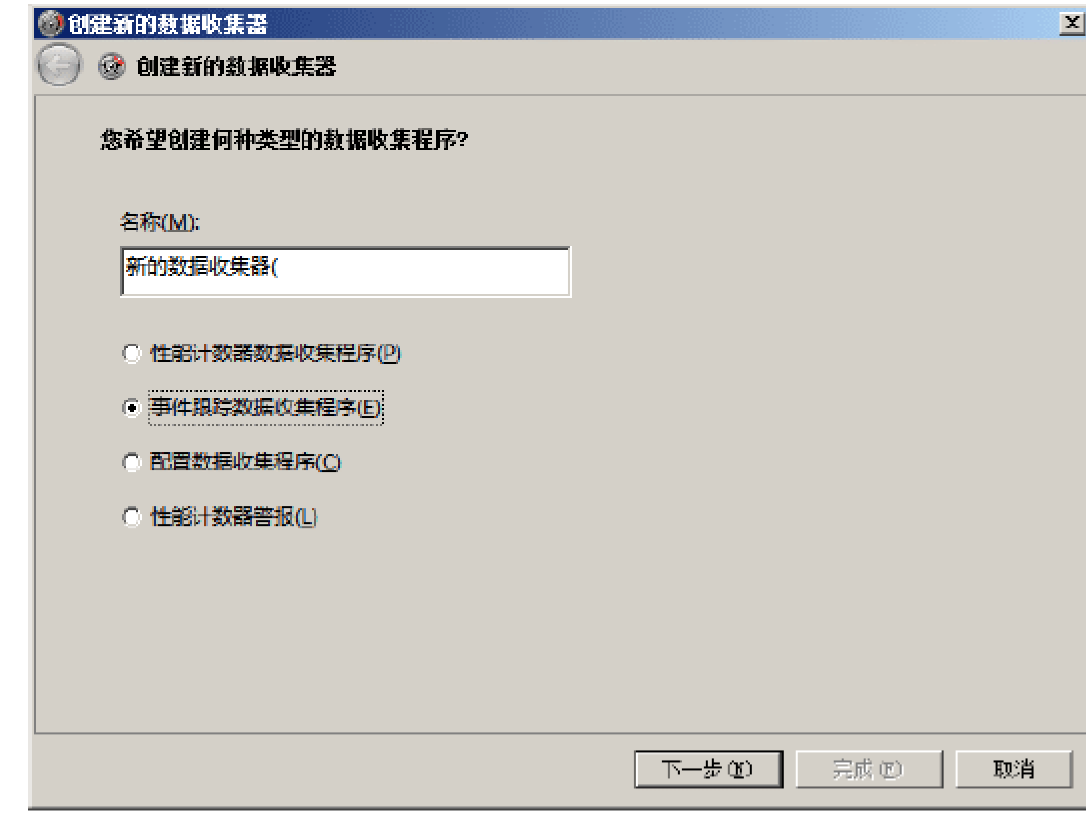


图 9-67　“您希望创建何种类型的数据收集程序”界面

3. 添加性能计数器

创建数据收集器过程中已经添加了相关的性能计数器，数据收集器运行过程中，管理员可以按照如下操作步骤添加新的性能计数器。

① 在“可靠性和性能监视器”窗口的“数据收集器集”目录中，展开相关的数据收集器集，并双击其中需要添加性能计数器的数据收集器，如“监视磁盘工作状态”数据收集器集中的“系统监视器日志”，打开如图 9-68 所示的“系统监视器日志 属性”对话框。

② 在“性能计数器”选项卡中，单击“添加”按钮打开如图 9-69 所示的对话框，从“可用计数器”列表中选择需要添加的计数器，并单击“添加”按钮添加到右侧列表中。



图 9-68 “系统监视器日志 属性”对话框

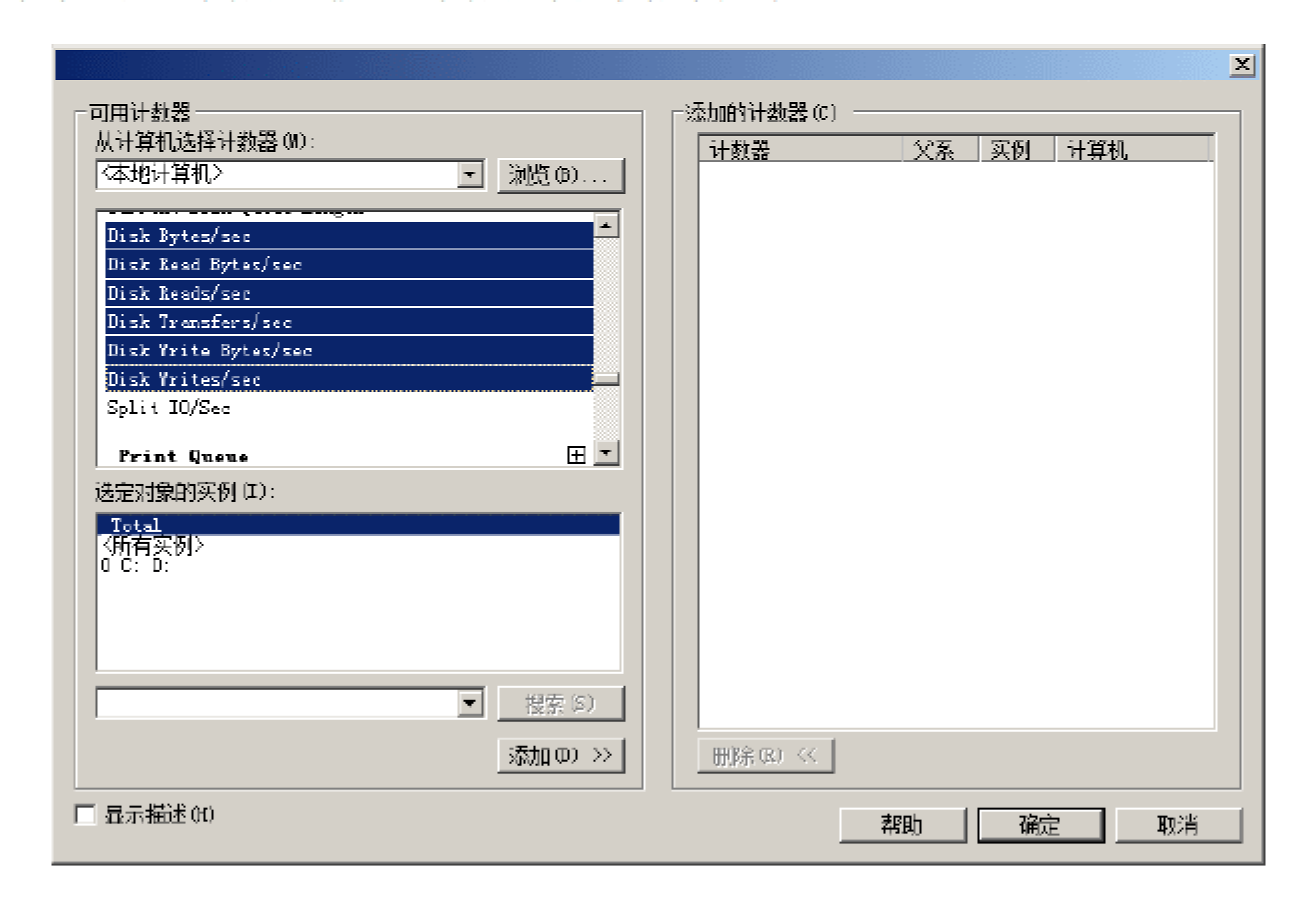


图 9-69 添加计数器

③ 单击“确定”按钮，即可将其添加到“性能计数器”列表中，如图 9-70 所示。

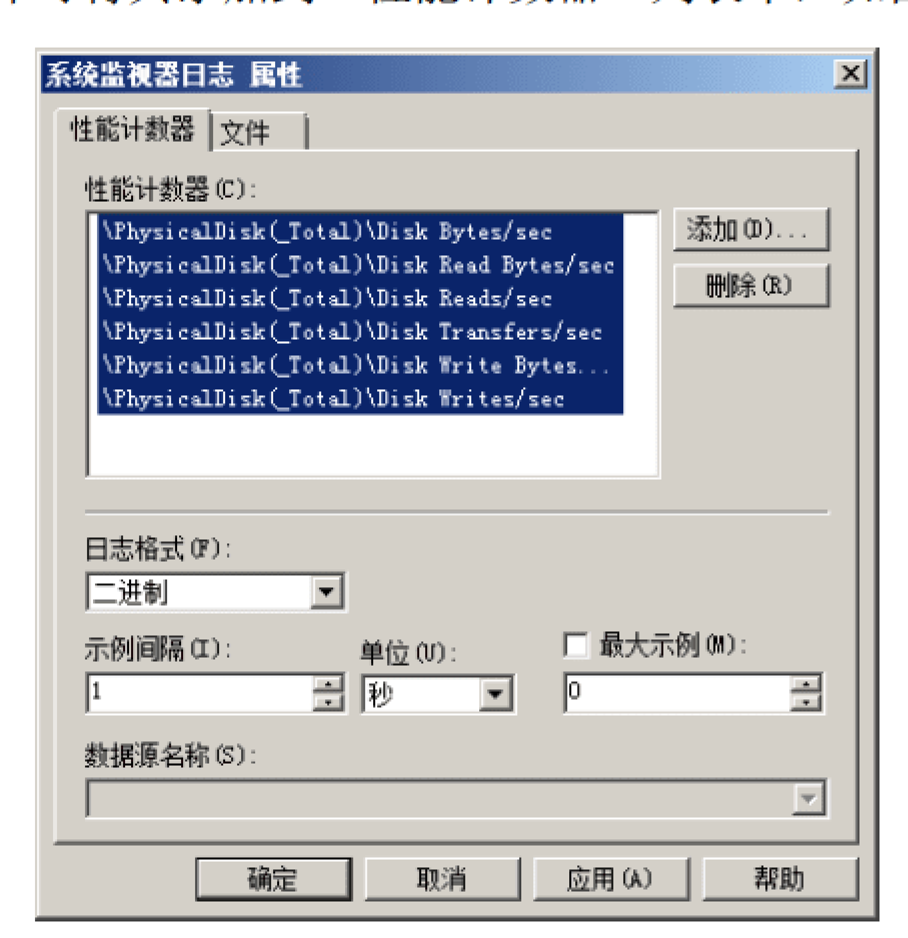


图 9-70 “性能计数器”选项卡

④ 切换至如图 9-71 所示的“文件”选项卡，在“日志文件名”文本框中可以重新输入新的文件名，在“文件名格式”文本框中单击右侧按钮，可以根据需要选择适当的命名格式，以便日后可以快速、准确查询所需的日志，例如以日志文件创建的日期、时间作为文件名的结尾。

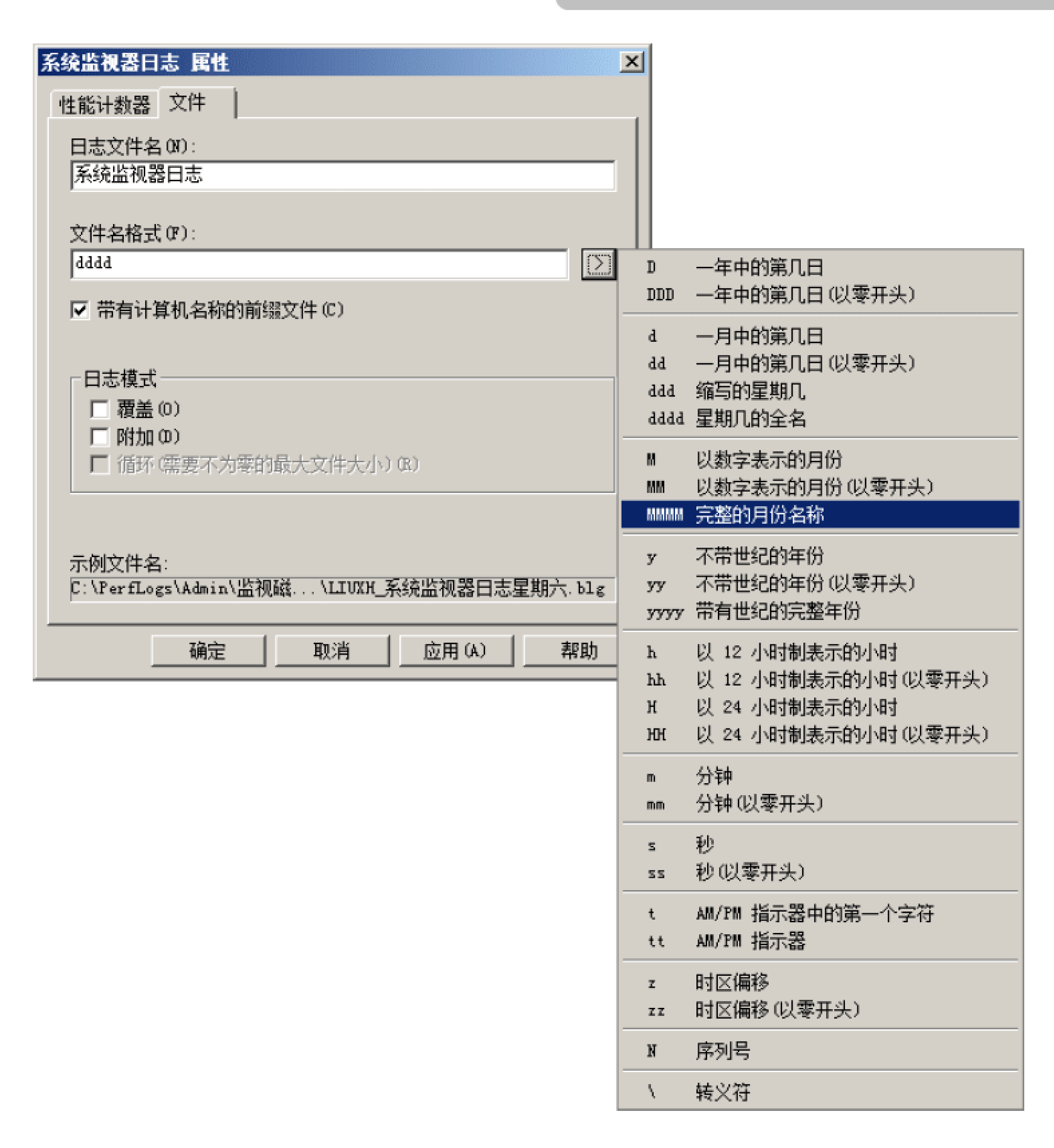


图 9-71　“文件”选项卡

⑤　单击“确定”按钮，保存设置即可。

9.3.3　报告

“报告”功能是 Windows Server 2008 系统可靠性和性能监视器的新增功能之一，主要用于直观反映数据收集器集的工作状态和结果。默认情况下，所有数据收集器集都可以在“报告”项目中，找到与之对应的数据收集器集报告。使用“报告”功能时，应注意如下几个方面。

- 如果数据收集器集未运行，将没有可用的报告。
- 如果数据收集器集正在运行，则控制台窗口中将显示有关数据收集器集被配置为运行多长时间的信息，无法查看历史记录。
- 数据收集停止之后，生成报告时会有一段延迟。这段时间期间，控制台窗口将显示工作图标。
- 较大的日志文件将使生成报告的时间较长。如果频繁检查日志以查看最新数据，建议使用限制以自动分段日志。可以使用 relog 命令对长日志文件进行分段或合并多个短日志文件。

在“可靠性和性能监视器”窗口中，展开“报告”→“用户定义”，即可查看自定义的数据收集器的报告信息。事件跟踪数据和配置信息数据的报告将以摘要方式显示，如图 9-72 所示。单击摘要名称即可显示或隐藏相关详细信息。



图 9-72　摘要方式显示的报告

性能计数器数据日志则以曲线图方式显示，如图 9-73 所示。除直接在“报告”窗口中查看相关日志，管理员也可以在“数据收集器集”中将性能日志文件导出，通过性能监视器浏览，效果完全相同。

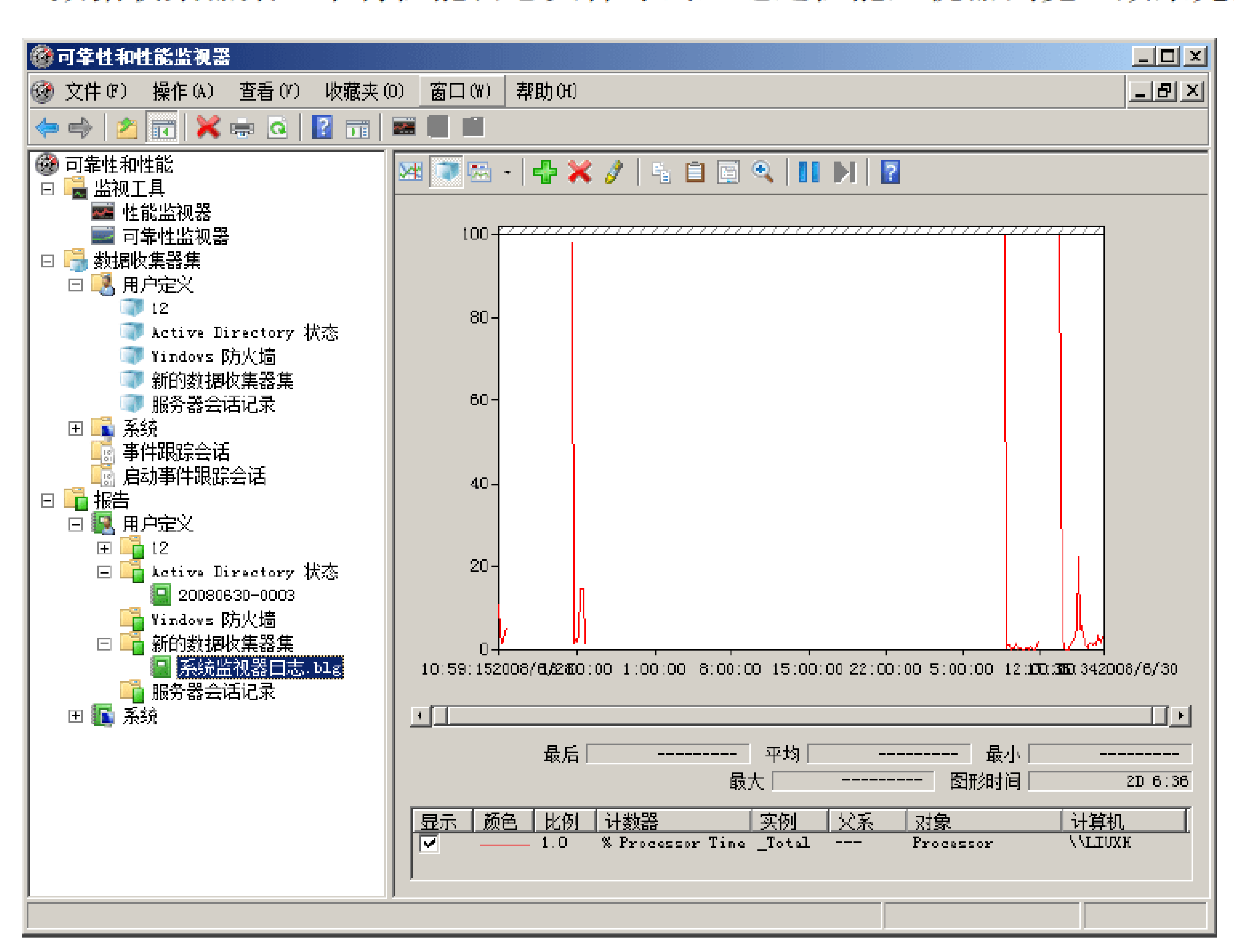


图 9-73　曲线图方式显示的报告

第 10 章　数 字 证 书

数字证书(Digital Certificate)是一种用于计算机身份认证的安全识别机制，是身份认证机构在数字身份证上的一个签名，这一行为表示身份认证机构已认定这个持证人的有效性。持有者可以凭借数字证书向计算机系统认证自己的身份，从而取得计算机或者某项服务的使用权。在获得数字证书后，可以将其保存在电脑里，也可以保存在 IC 卡或 USB Key 中，建议妥善保存，以免泄露。

关键词

- 数字证书服务的安装
- CA 证书的创建与安装
- CA 证书的管理与应用

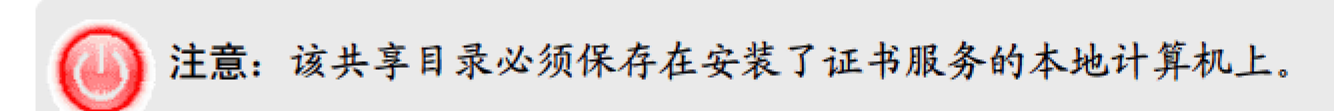
10.1 数字证书服务的安装

Windows Server 2008 的证书服务为管理员提供了发布、安装和撤销数字证书的能力。默认情况下，数字证书服务并不是系统的基本安装组件，在需要使用数字证书时，需要手动安装数字证书服务。

10.1.1 数字证书服务安装前的准备

在开始安装证书服务之前，应当首先做好如下工作。

- 必须建立一个共享文件夹，将权限设置为读取，并指定允许访问该文件夹的用户，用于为证书服务保存 Certificate Authority 证书和各种配置文件，以便客户能够通过网络访问和安装 CA 证书。



注意：该共享目录必须保存在安装了证书服务的本地计算机上。

- 若欲创建企业根 CA 或企业从属 CA，应当首先配置好活动目录(Active Directory)。若欲创建独立根 CA 或独立从属根 CA，则无需配置 Active Directory。

10.1.2 数字证书服务的安装

Windows Server 2008 支持两种证书服务，分别是用于企业内部的企业证书服务器(企业 CA)和用于企业或 Internet 网络中的独立的证书服务器(独立 CA)。企业 CA 需要 Windows Server 2008 活动目录的支持，而独立 CA 则可以安装在任何独立的 Windows Server 2008 计算机中。

1. 企业 CA 的安装

证书服务作为 Windows Server 2008 的内置组件，默认情况下并没有安装。由于企业证书服务需要活动目录的支持，因此，在安装企业证书服务时必须先安装域服务。

① 运行“添加角色向导”，在如图 10-1 所示的“选择服务器角色”界面中，在“角色”列表框中选中“Active Directory 证书服务”复选框。



图 10-1 “选择服务器角色”界面

② 单击“下一步”按钮，显示如图 10-2 所示的“Active Directory 证书服务简介”界面，其中显示了证书服务的简介及注意事项。

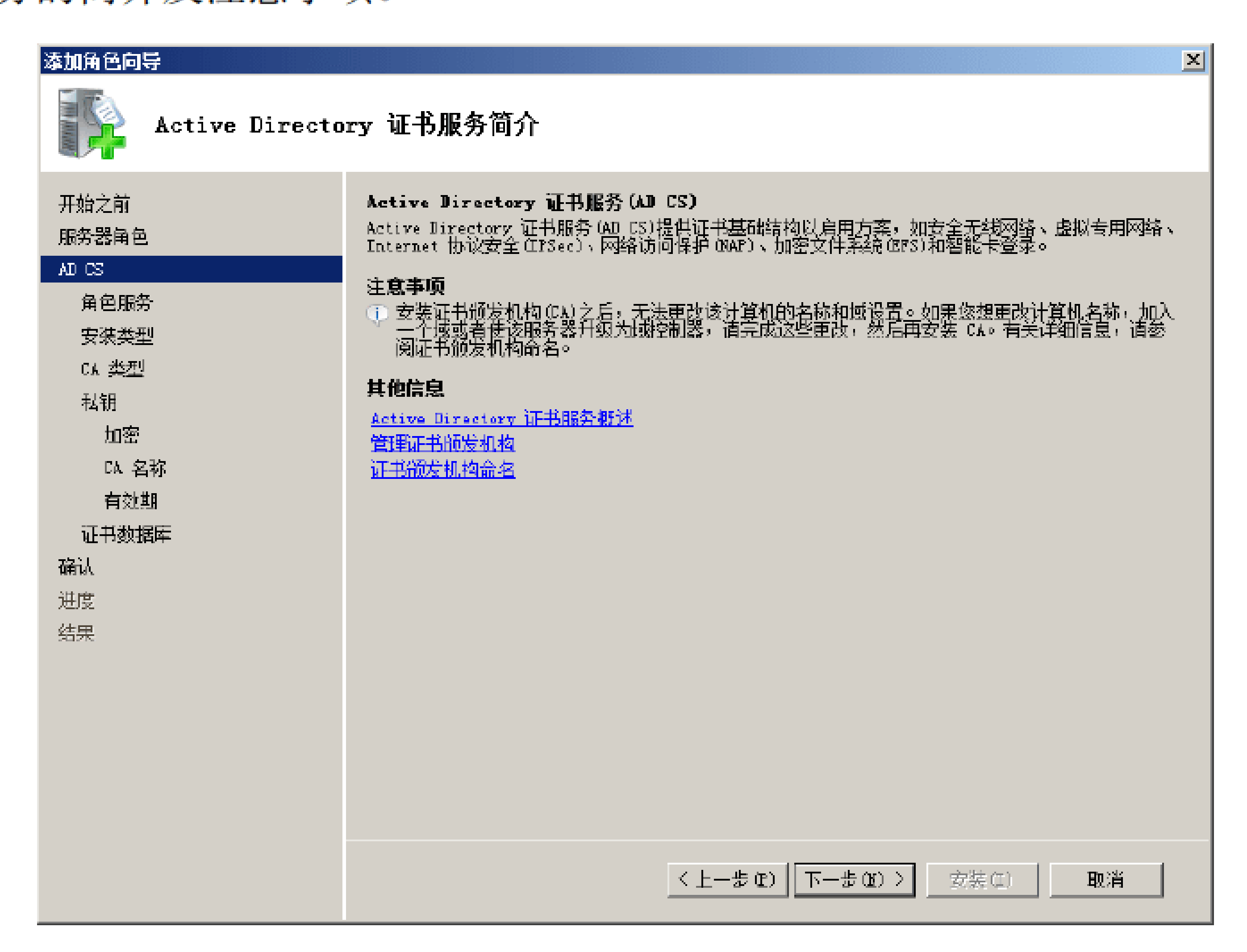


图 10-2　“Active Directory 证书服务简介”界面

③ 单击“下一步”按钮，显示如图 10-3 所示的“选择角色服务”界面。选择为 Active Directory 证书服务安装的角色服务，默认选中“证书颁发机构”复选框。



图 10-3　“选择角色服务”界面

④ 如果要启用证书 Web 注册功能，可同时选中“证书颁发机构 Web 注册”复选框。显示如图 10-4 所示的对话框，添加 Web 服务器功能。

注意：只有 Windows Server 2008 企业版和数据中心版支持 Web 注册功能，标准版和 Web 版则不支持。

⑤ 单击“添加必需的角色服务”按钮，显示如图 10-5 所示的“指定安装类型”界面。选择“企业”单选按钮，用来安装企业证书。

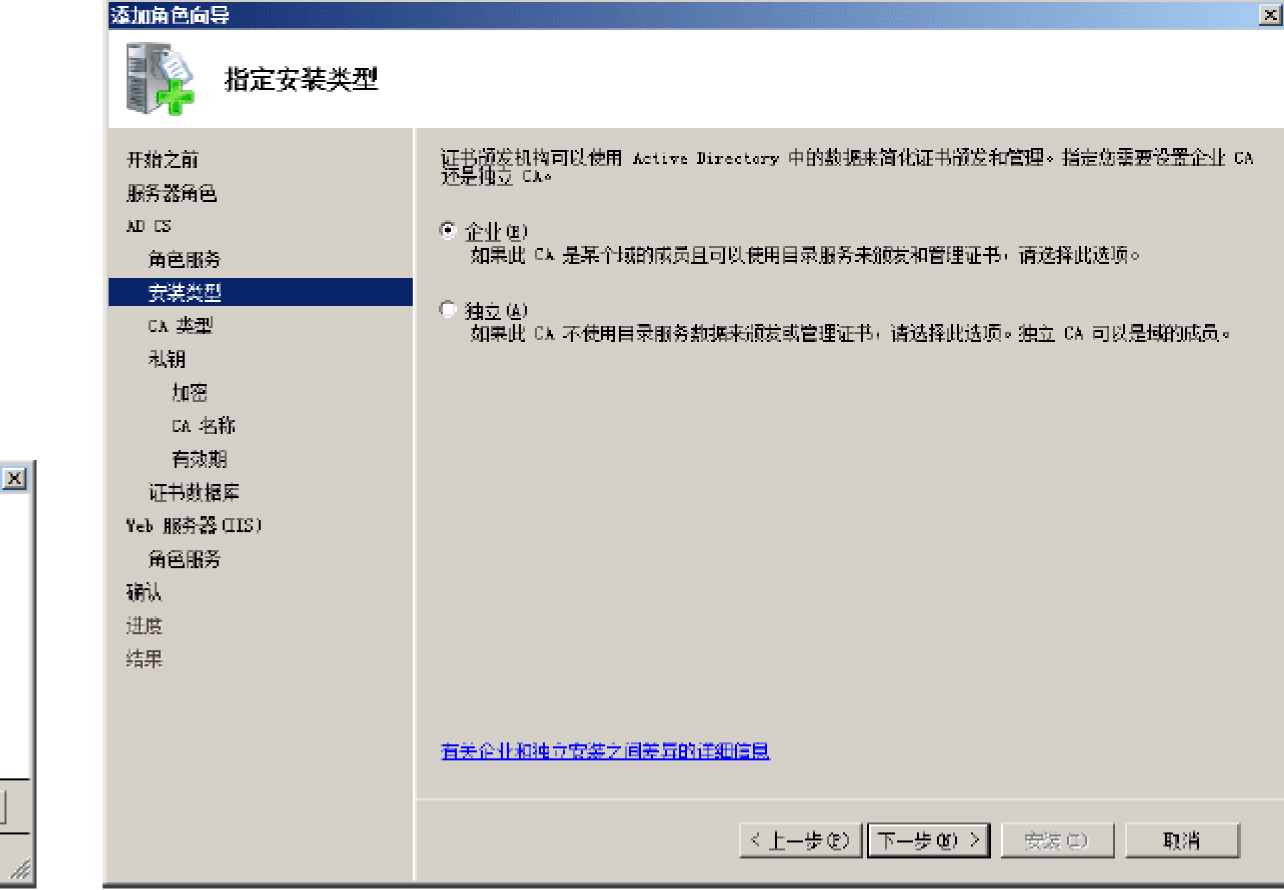


图 10-4 添加 Web 功能　　　　图 10-5 “指定安装类型”界面

⑥ 单击“下一步”按钮，显示如图 10-6 所示的“指定 CA 类型”界面。由于是第一次安装，并且是唯一的证书颁发机构，因此，选择“根 CA”单选按钮。

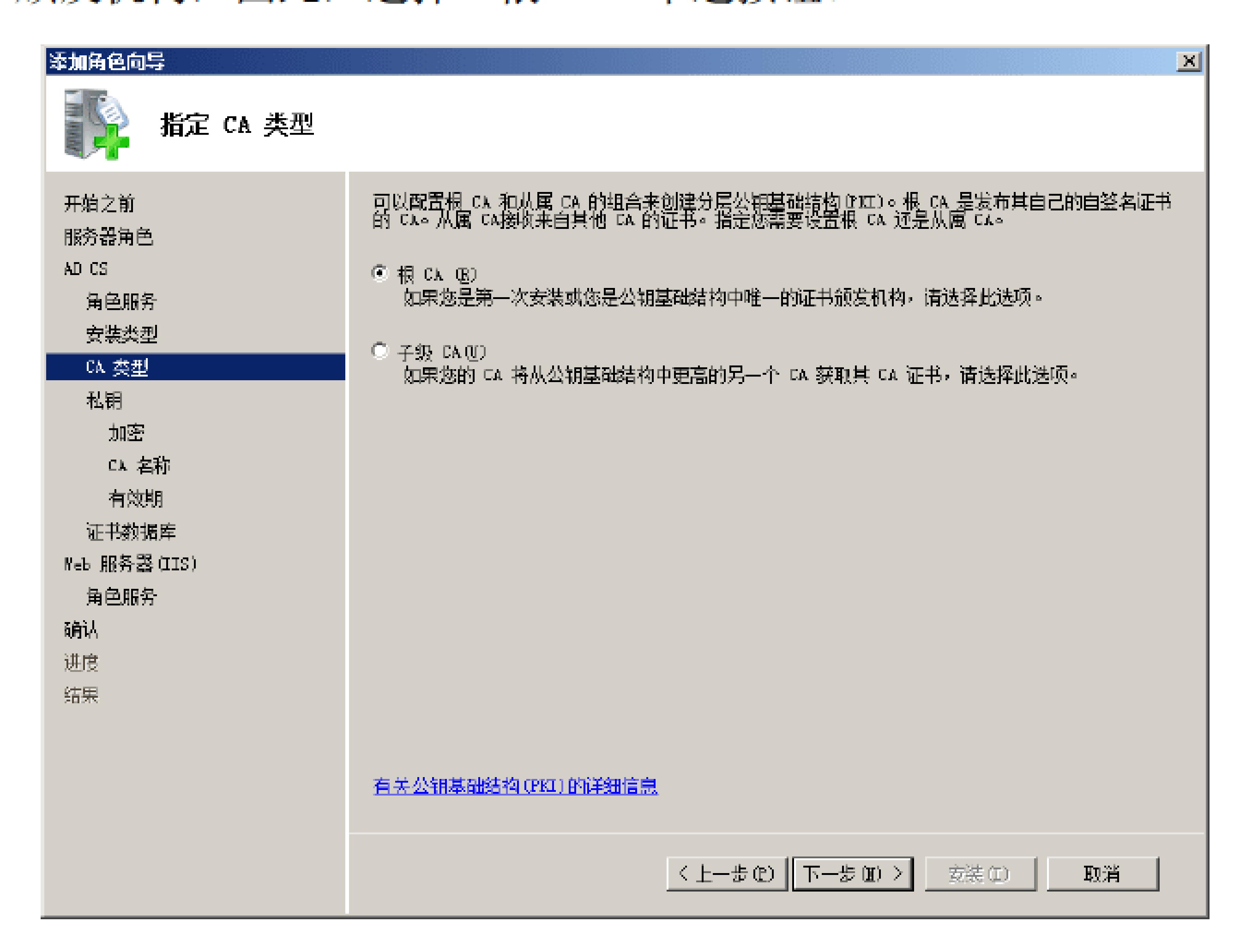


图 10-6 “指定 CA 类型”界面

⑦ 单击“下一步”按钮，显示如图 10-7 所示的“设置私钥”界面。由于现在是第一次安装证书服务，且没有私钥，因此，选择“新建私钥”单选按钮。

⑧ 单击“下一步”按钮，显示如图 10-8 所示的“为 CA 配置加密”界面。在“选择加密服务提供程序”下拉列表框中，选择加密程序；在“密钥字符长度”下拉列表框中选择密钥长度；在“选择此 CA 颁发的签名证书的哈希算法”列表框中，选择要使用的哈希算法。

⑨ 单击“下一步”按钮，显示如图 10-9 所示的“配置 CA 名称”界面，在“此 CA 的公用名称”文本框中设置此证书的公用名称。



图 10-7 “设置私钥”界面

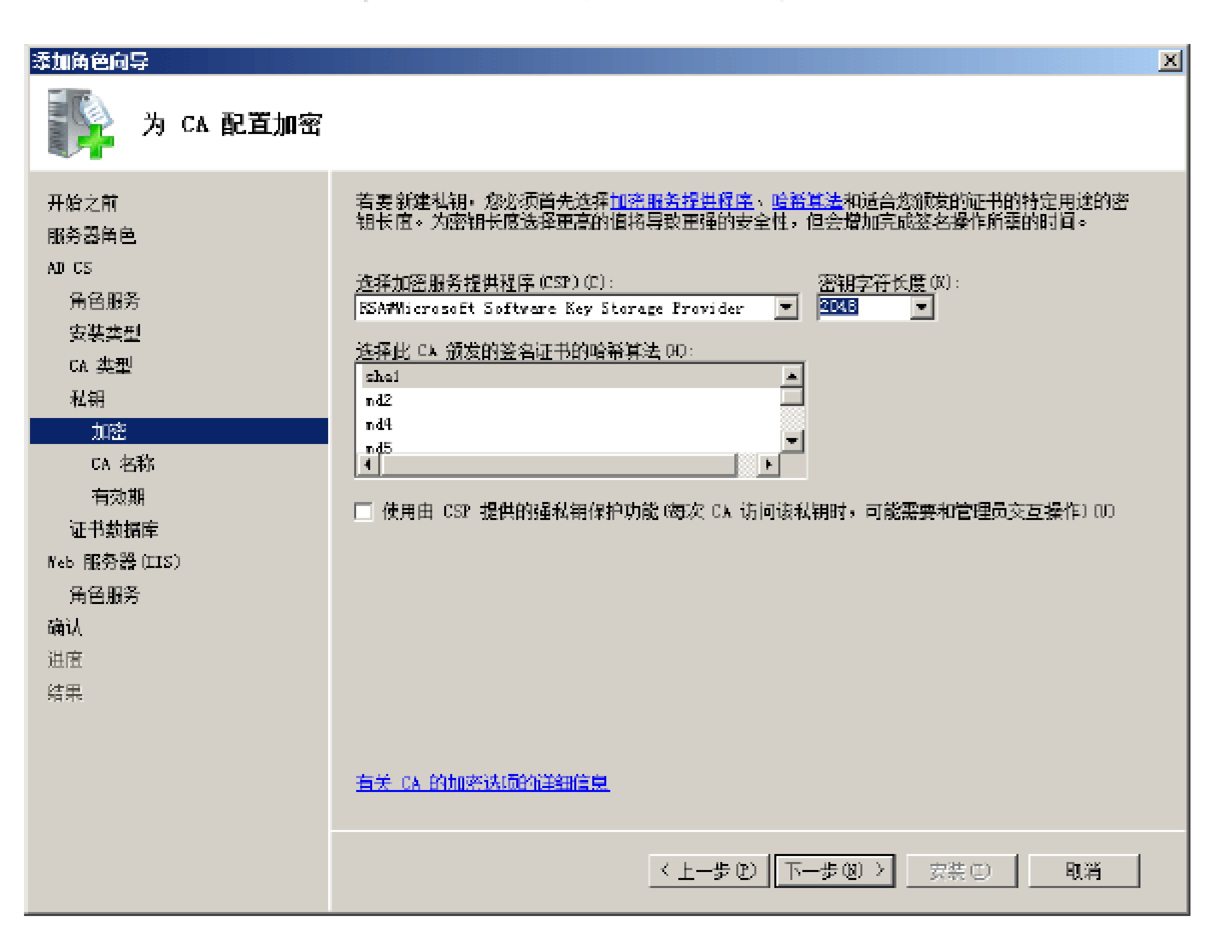


图 10-8 “为 CA 配置加密”界面



图 10-9 “配置 CA 名称”界面

⑩ 单击“下一步”按钮，显示如图 10-10 所示的“设置有效期”界面。设置该证书的有效期，默认为 5 年。

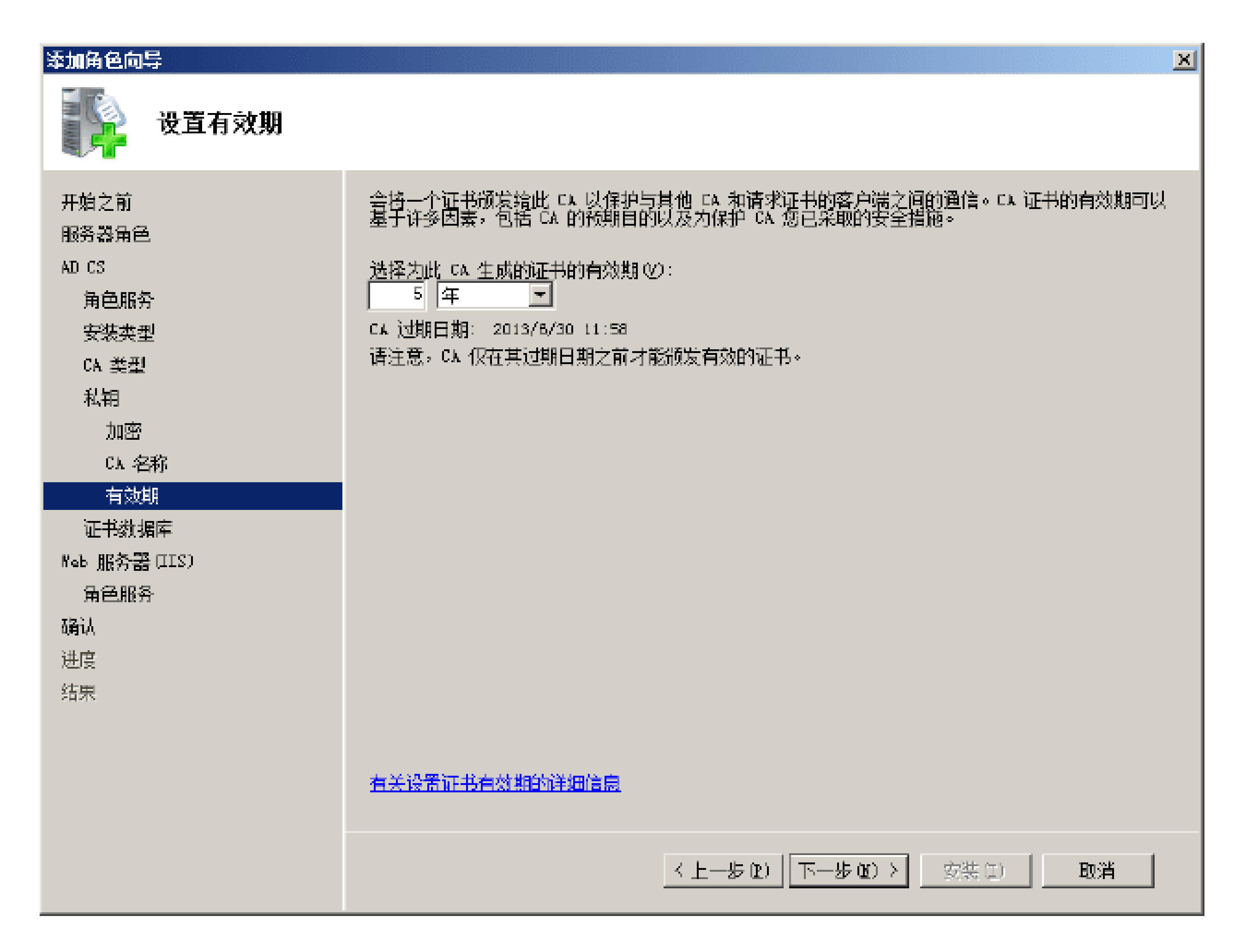


图 10-10 “设置有效期”界面

⑪ 单击“下一步”按钮，显示如图 10-11 所示的“配置证书数据库”界面，用来设置证书数据库和数据库日志的位置。

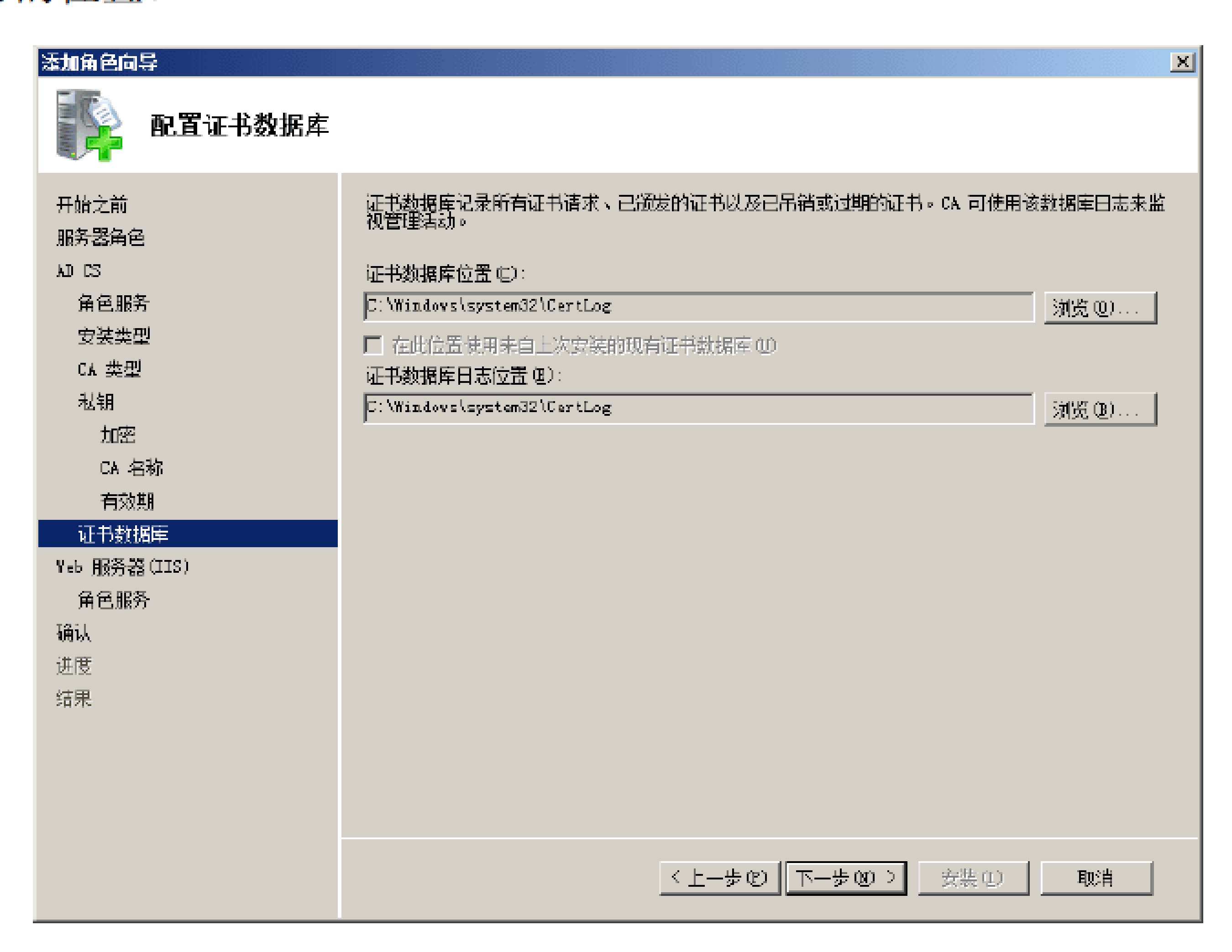


图 10-11 “配置证书数据库”界面

⑫ 由于要同时安装“证书颁发机构 Web 注册”功能，单击“下一步”按钮，显示如图 10-12 所示的“Web 服务器(IIS)”界面，其中显示了 IIS 的简介信息。

⑬ 单击“下一步”按钮，显示如图 10-13 所示的“选择角色服务”界面。选择欲安装的 IIS 组件，通常保持默认设置即可。

⑭ 单击“下一步”按钮，显示如图 10-14 所示的“确认安装选择”界面。其中显示欲安装的角色；同时提示用户当安装了证书服务以后，将无法更改计算机的名称和域设置。



图 10-12 “Web 服务器(IIS)”界面

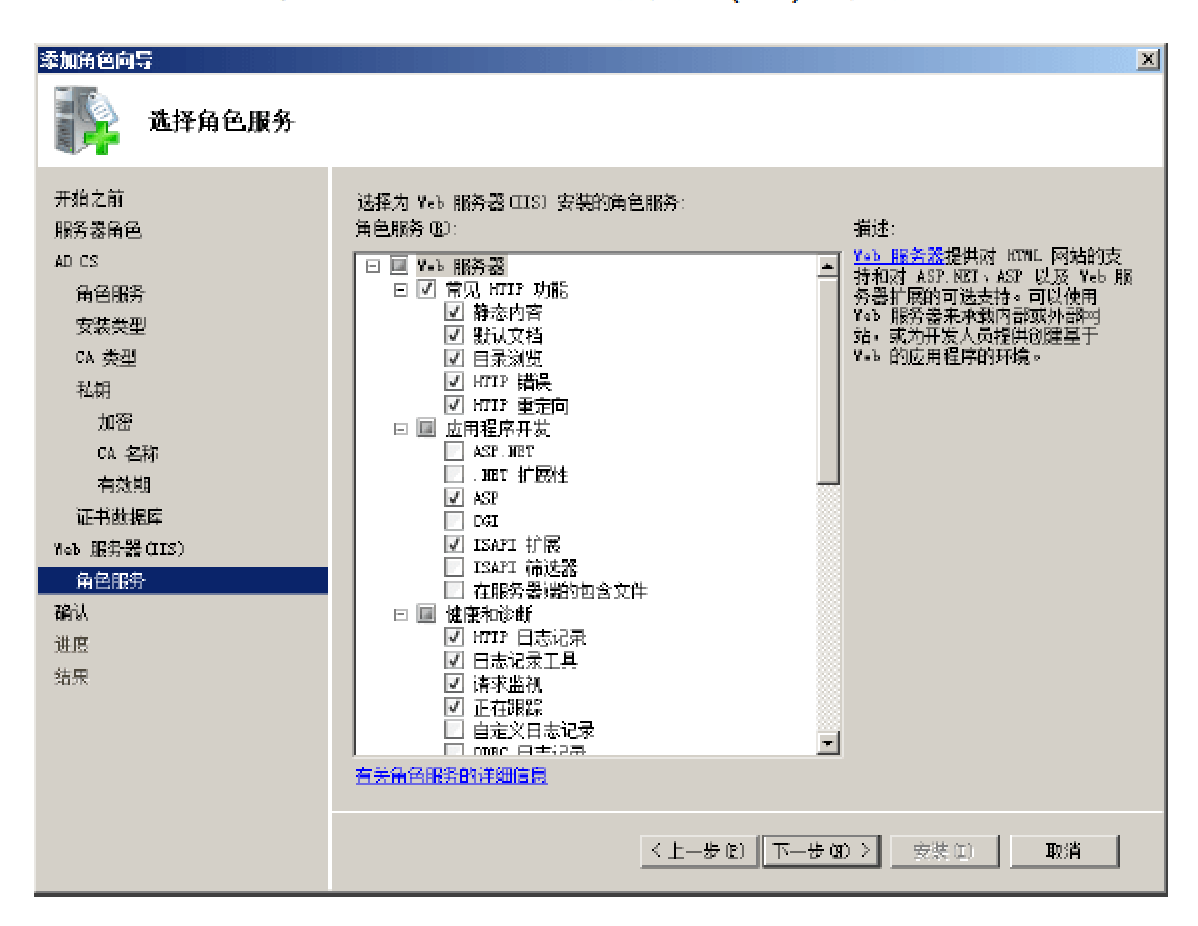


图 10-13 “选择角色服务”界面



图 10-14 “确认安装选择”界面

⑮ 单击“安装”按钮，开始安装证书服务及相关组件。安装完成以后，显示如图 10-15 所示的“安装结果”界面。



图 10-15 “安装结果”界面

⑯ 单击“关闭”按钮，证书服务安装完成。

打开“服务器管理器”窗口，依次展开“角色”→“Active Directory 证书服务”选项，即可查看所安装的证书服务，如图 10-16 所示。

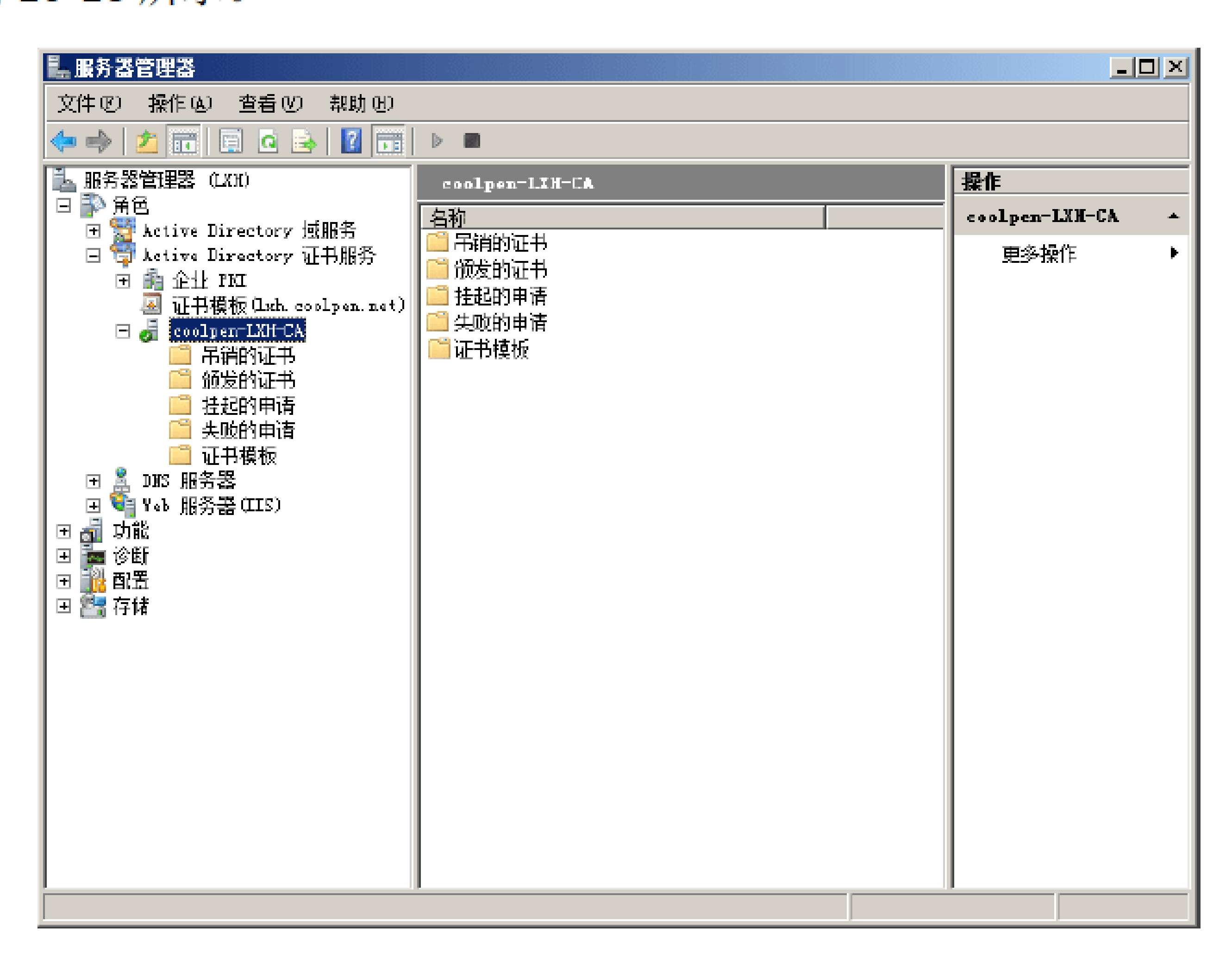


图 10-16 证书服务

2. 独立根 CA 的安装

如果网络内尚未安装域服务，可以将证书服务安装在独立服务器上，从而实现证书的颁发与管理。不过，由于独立根 CA 不需要 Active Directory，因此，只能使用 Web 方式注册证书，无法使用“证书申请向导”，而且所申请的证书必须由管理员颁发。

① 以管理员用户身份登录到服务器，运行“添加角色向导”，在“选择服务器角色”对话框中选中“Active Directory 证书服务”复选框。

② 在“选择角色服务”界面中，同时选中“证书颁发机构”和“证书颁发机构 Web 注册”复选框，以启用 Web 注册功能，如图 10-17 所示。

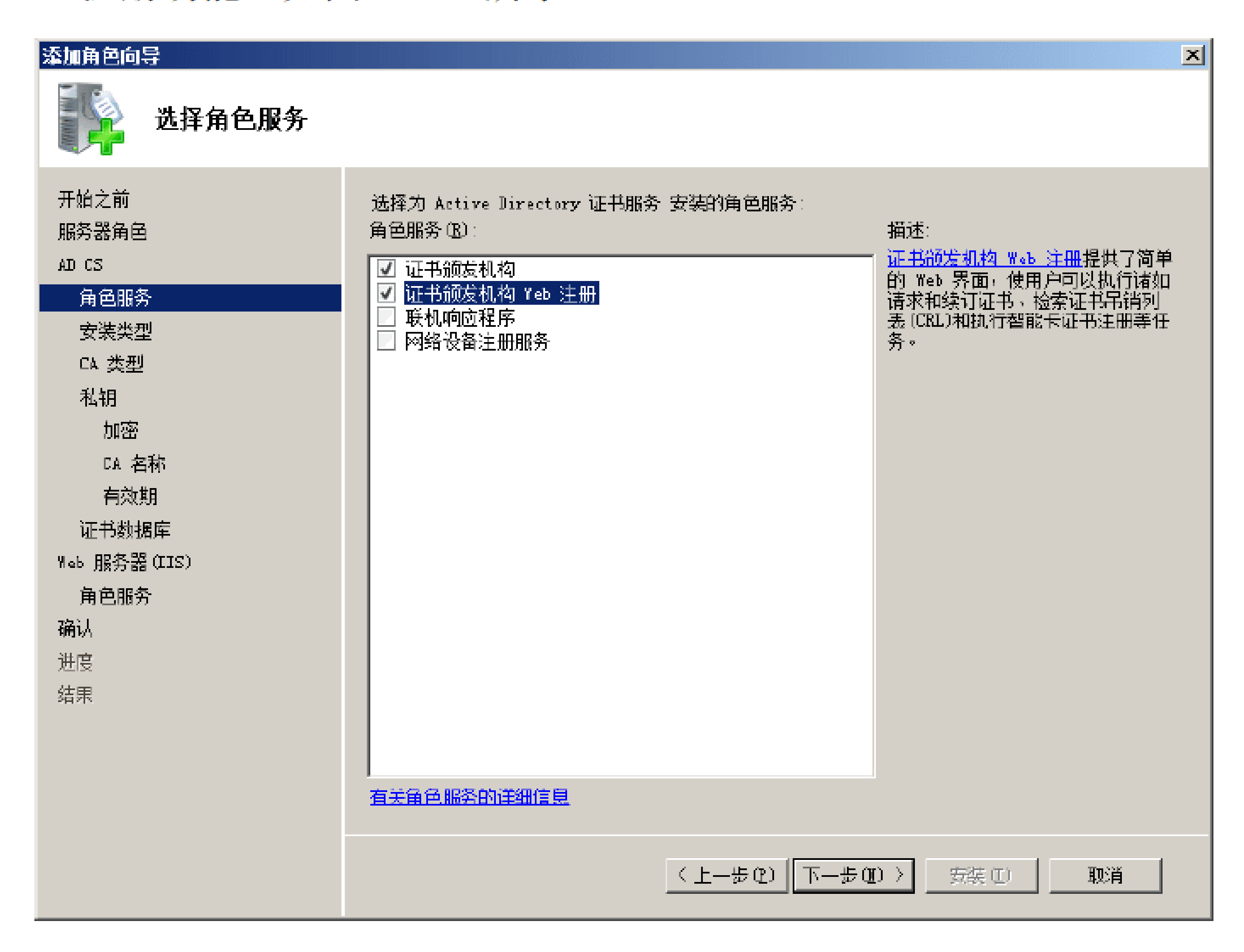


图 10-17　“选择角色服务”界面

③ 在“指定安装类型”界面中，选择“独立”单选按钮，如图 10-18 所示。由于此服务器不是域控制器，且未加入域，因此，“企业”单选按钮为灰色不可选状态。

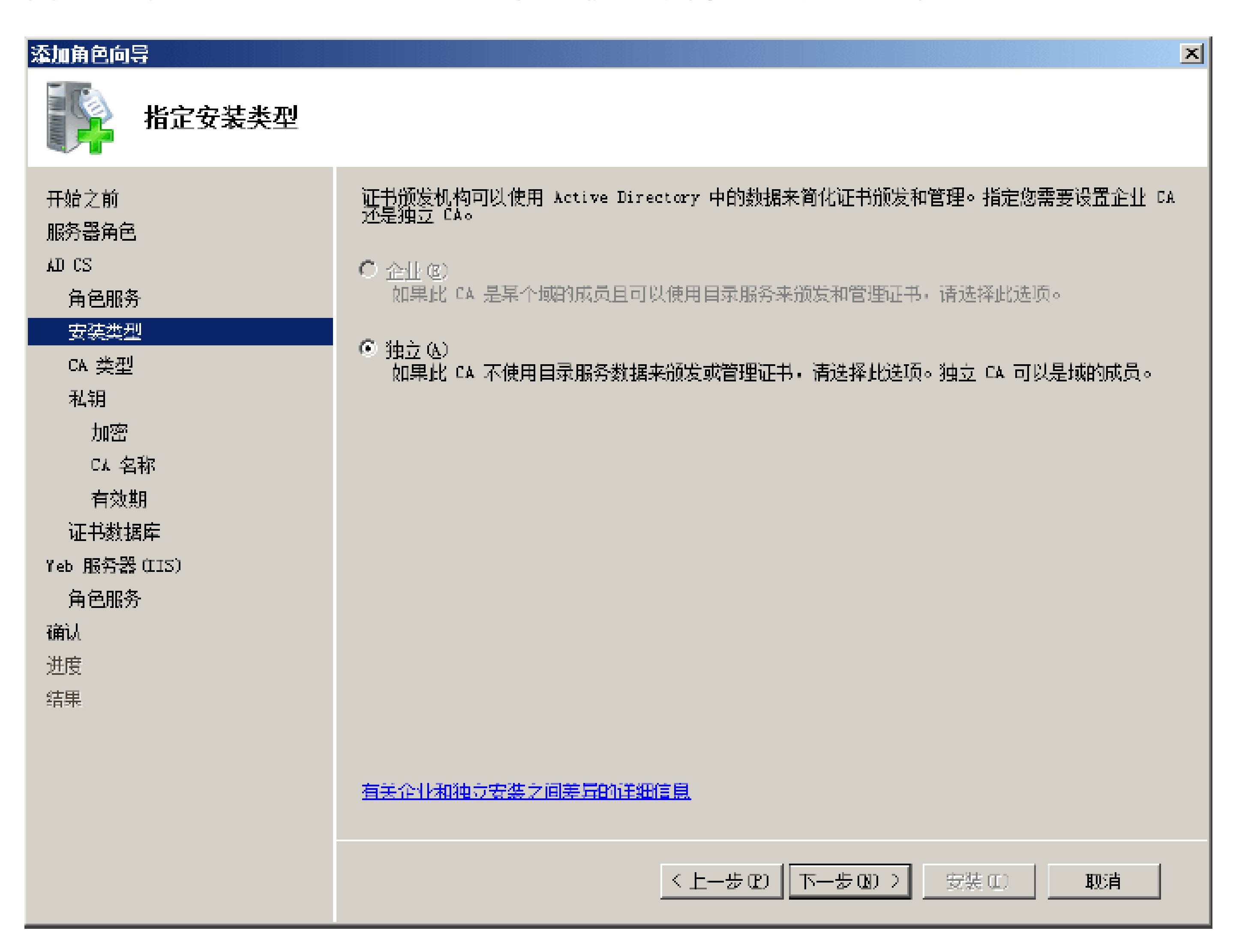


图 10-18　“指定安装类型”界面

④ 其他操作与安装企业 CA 时完全相同，这里不再赘述。

10.2 CA 证书的创建与安装

证书服务器安装完成后，企业中的用户都可以申请证书，无论是域成员用户，还是非域成员，都可以向证书服务器申请证书。申请证书可以使用 Web 方式或“证书申请向导”两种方式，前者适用于所有用户，而后者则需要用户加入域才能使用。

10.2.1 服务端 CA 证书的创建

服务端 CA 证书的申请可以通过 Web 方式和“证书申请向导”方式进行，对于没有加入域的计算机则可以通过 Web 方式进行数字证书的申请；对于加入域的计算机可以通过 Web 方式和“证书申请向导”两种方式申请数字证书。

1. 使用 Web 方式申请与安装证书

如果在安装证书服务器的同时也安装了“证书颁发机构 Web 注册”，那么，就可以通过 Web 方式来申请证书，而且不需要加入域，但需要配置信任证书服务器才能安装证书。而对于域用户，则无须配置证书服务信任即可安装证书。申请证书的客户端可以使用 Windows 2000/XP/Vista 操作系统，下面以 Windows Vista 系统为例进行介绍。

(1) 配置 IE 浏览器

① 使用管理员用户登录 Windows Vista，首先需要使 IE 浏览器运行 ActiveX 控件。打开 IE 浏览器，单击“工具”菜单中的“Internet 选项”命令，切换到“安全”选项卡，显示如图 10-19 所示。

② 单击“自定义级别”按钮，显示“安全设置 – Internet 区域”对话框，将“对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本(不安全)”和“允许运行以前未使用的 ActiveX 控件而不提示”均设置为“启用(不安全)”状态，如图 10-20 所示。

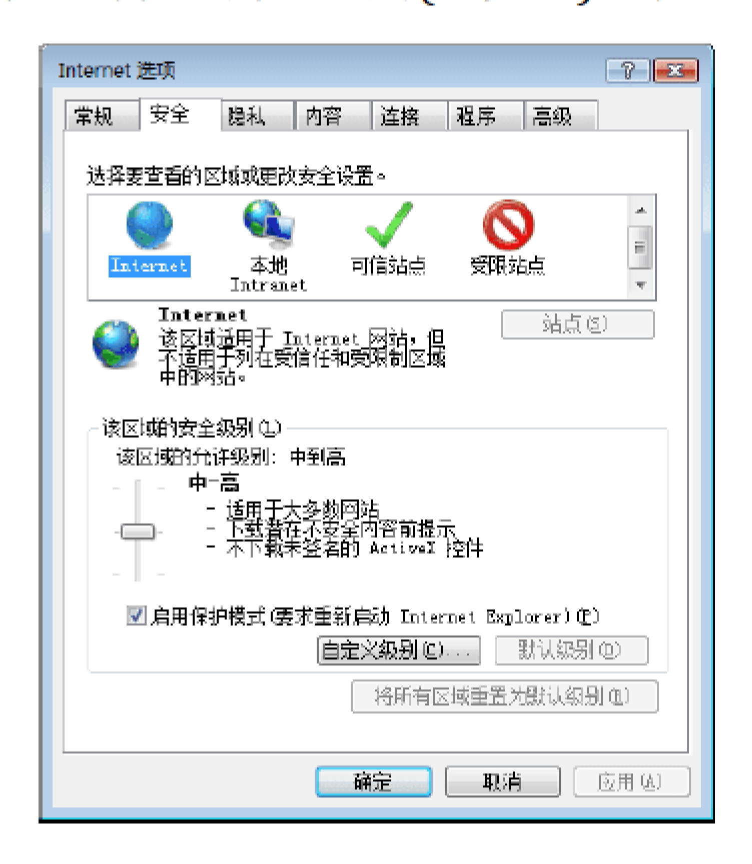



图 10-19 “Internet 选项”对话框

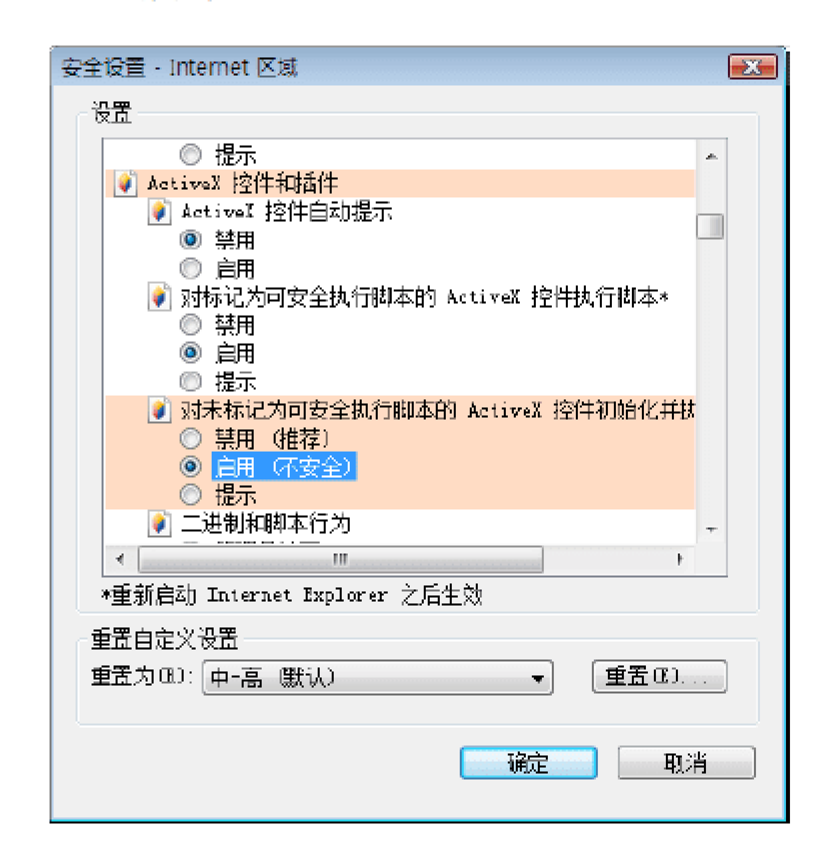


图 10-20 “安全设置 - Internet 区域”对话框


注意：如果未在 IE 浏览器的安全设置中启用这两项，则在申请证书时就会显示如图 10-21 所示的提示框。

③　单击“确定”按钮，保存设置即可。

(2)　信任证书颁发机构

如果客户端计算机没有加入域，则必须配置为信任证书颁发机构，才能安装从证书服务器申请的证书；否则，将无法安装。

①　打开 Web 浏览器，在地址栏中输入证书服务器的证书申请地址，格式为 http://证书服务器的 IP 地址/certsrv，例如“http://192.168.1.10/certsrv”，按 Enter 键确认，显示如图 10-22 所示的连接到登录框。

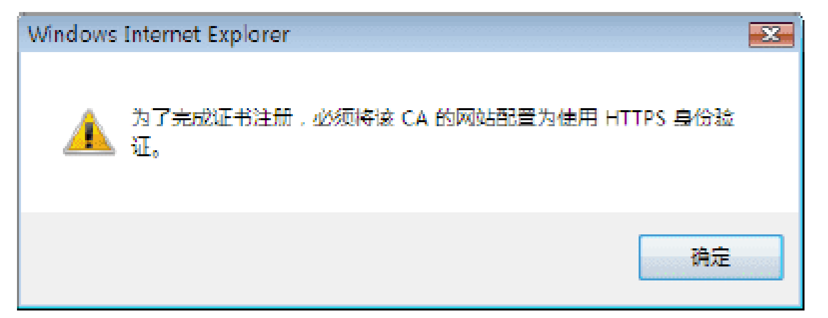


图 10-21　提示框

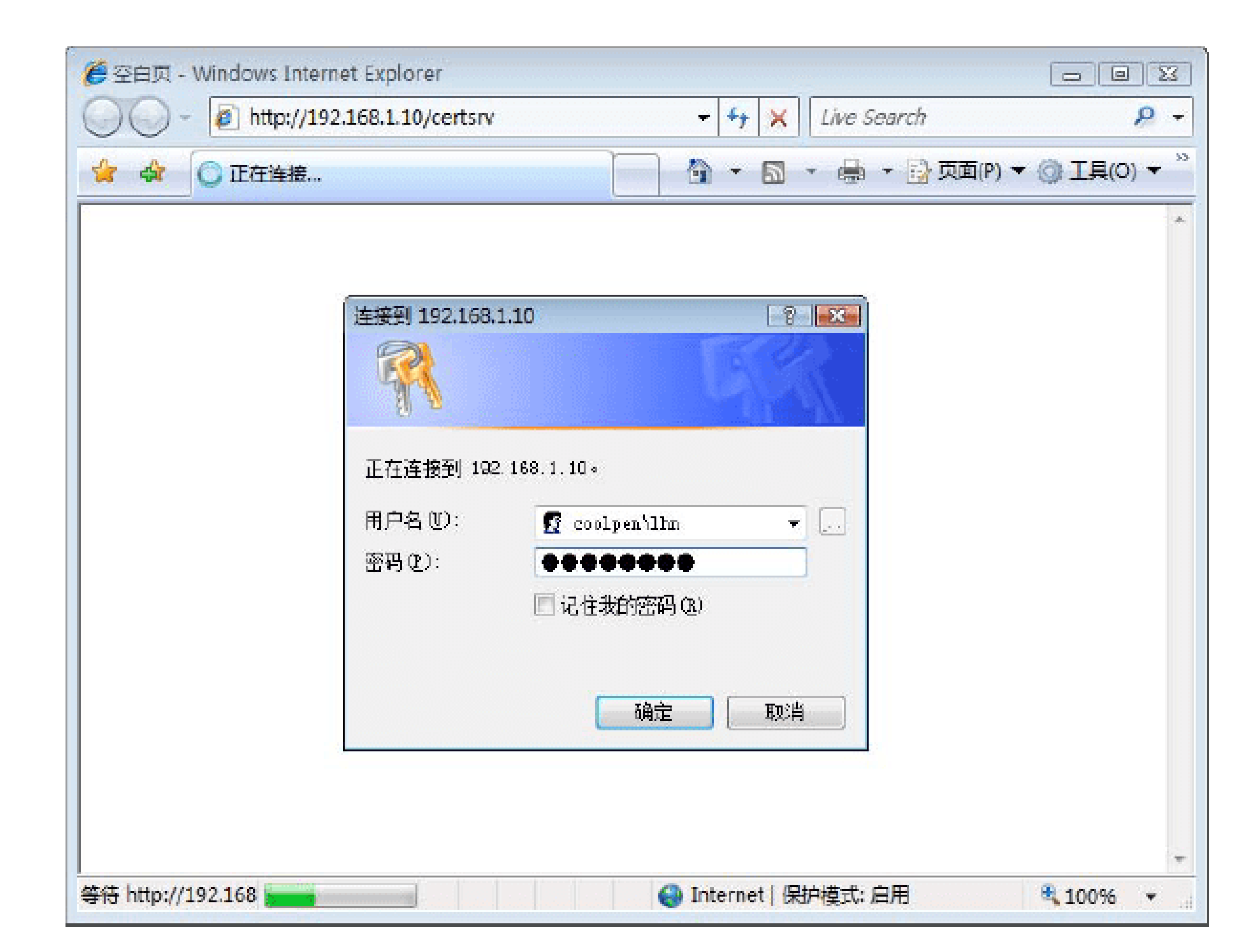


图 10-22　登录框

②　在“用户名”下表列表框和“密码”文本框中，分别输入具有登录证书服务器权限的用户名和密码，然后单击“确定”按钮，显示如图 10-23 所示的“Microsoft Active Directory 证书服务”窗口。



图 10-23　“Microsoft Active Directory 证书服务”窗口

③　单击“下载 CA 证书、证书链或 CRL”超级链接，显示如图 10-24 所示的“下载 CA 证书、证书链或 CRL”窗口，用来下载证书或证书链。

④ 单击“下载 CA 证书”链接，显示如图 10-25 所示的“文件下载”对话框。单击“保存”按钮，将该证书保存到本地计算机中。

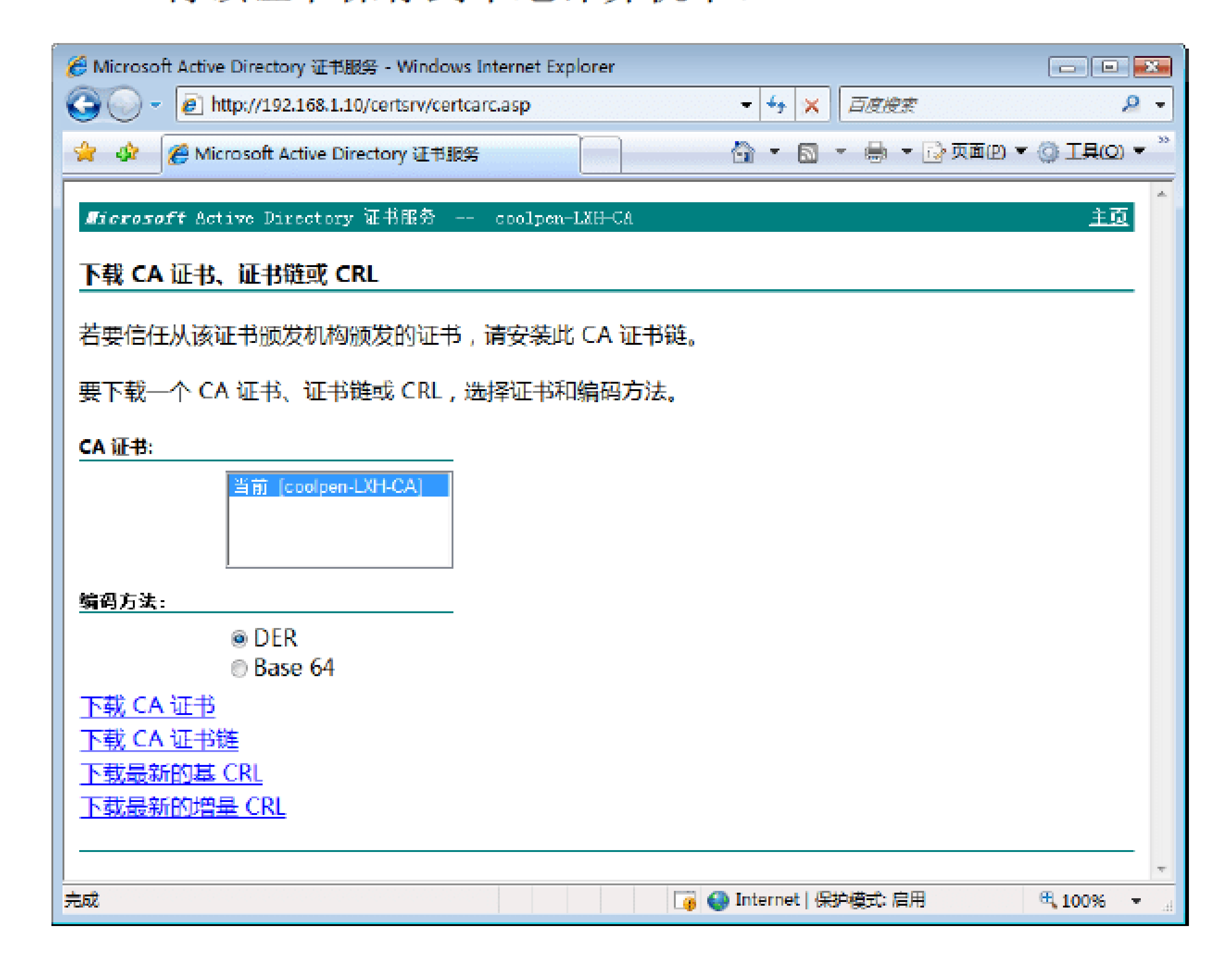


图 10-24 “下载 CA 证书、证书链或 CRL”窗口

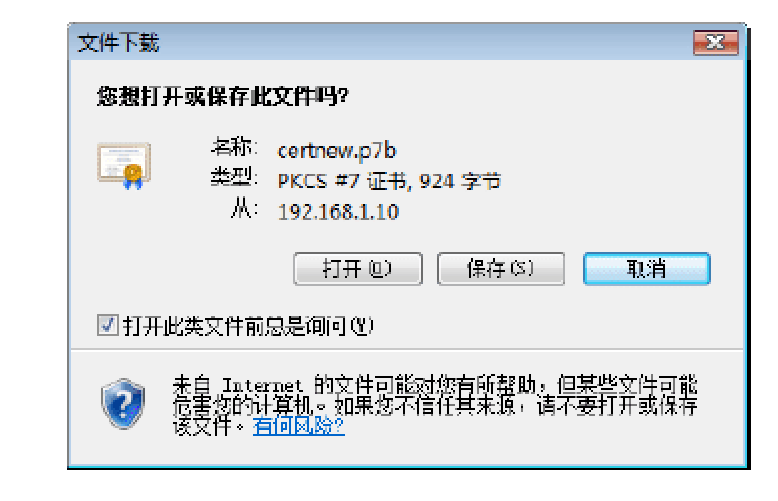


图 10-25 下载证书链

⑤ 证书下载完成以后，在 Windows 资源管理器中选择所下载的证书链文件，右击并选择快捷菜单中的“安装证书”命令，运行“证书导入向导”对话框，如图 10-26 所示。

⑥ 单击“下一步”按钮，显示如图 10-27 所示的“证书存储”界面，选择保存证书的系统区域。

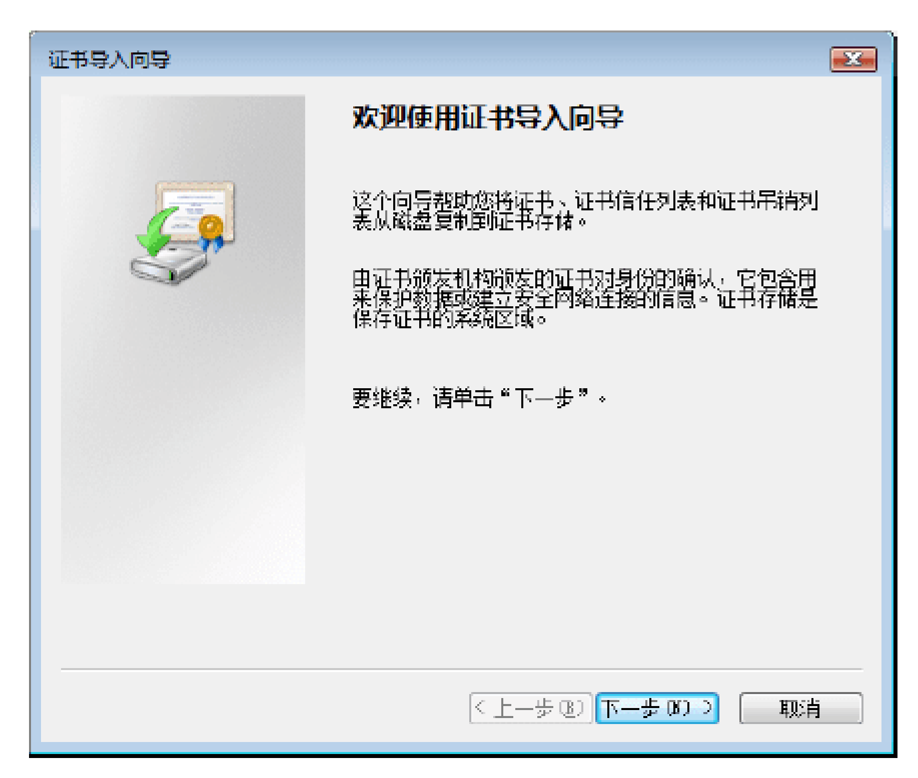


图 10-26 “证书导入向导”对话框

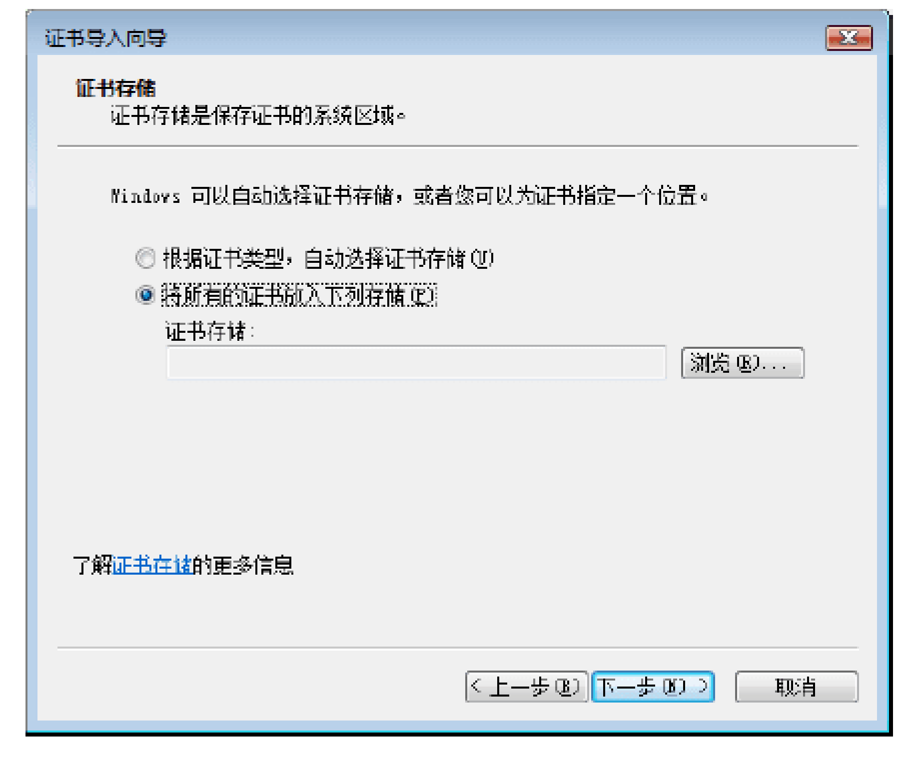


图 10-27 “证书存储”界面

⑦ 选择“将所有的证书放入下列存储”单选按钮，并单击“浏览”按钮，显示如图 10-28 所示的“选择证书存储”对话框。选择“受信任的根证书颁发机构”选项，然后单击“确定”按钮。

⑧ 单击“下一步”按钮，显示如图 10-29 所示的“正在完成证书导入向导”界面。

⑨ 单击“完成”按钮，显示如图 10-30 所示的“安全性警告”对话框，要求确认是否安装此证书。

⑩ 单击“是”按钮，显示如图 10-31 所示的提示框，提示证书导

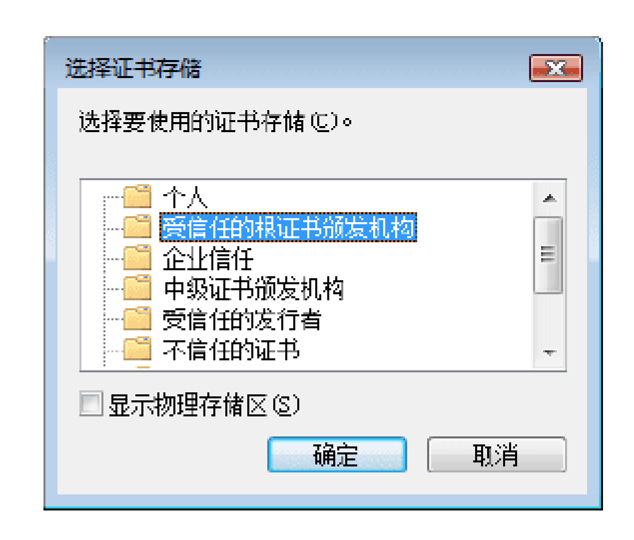


图 10-28 “选择证书存储”对话框

入成功。此时，即可开始颁发并安装证书。

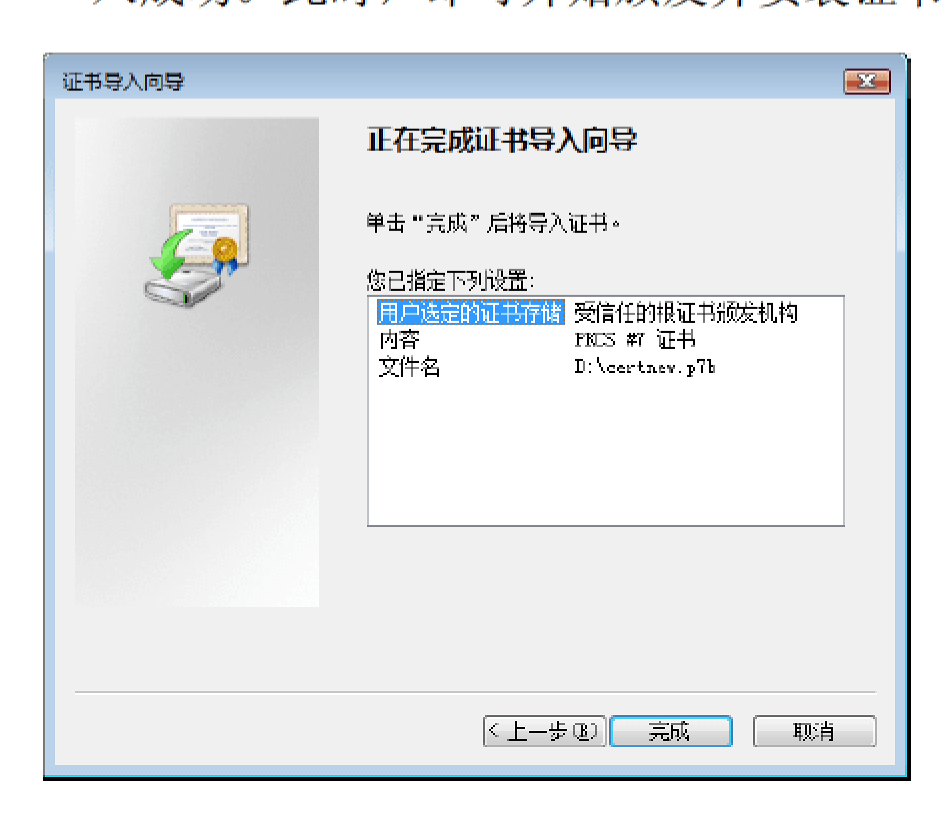


图 10-29　“正在完成证书导入向导”界面

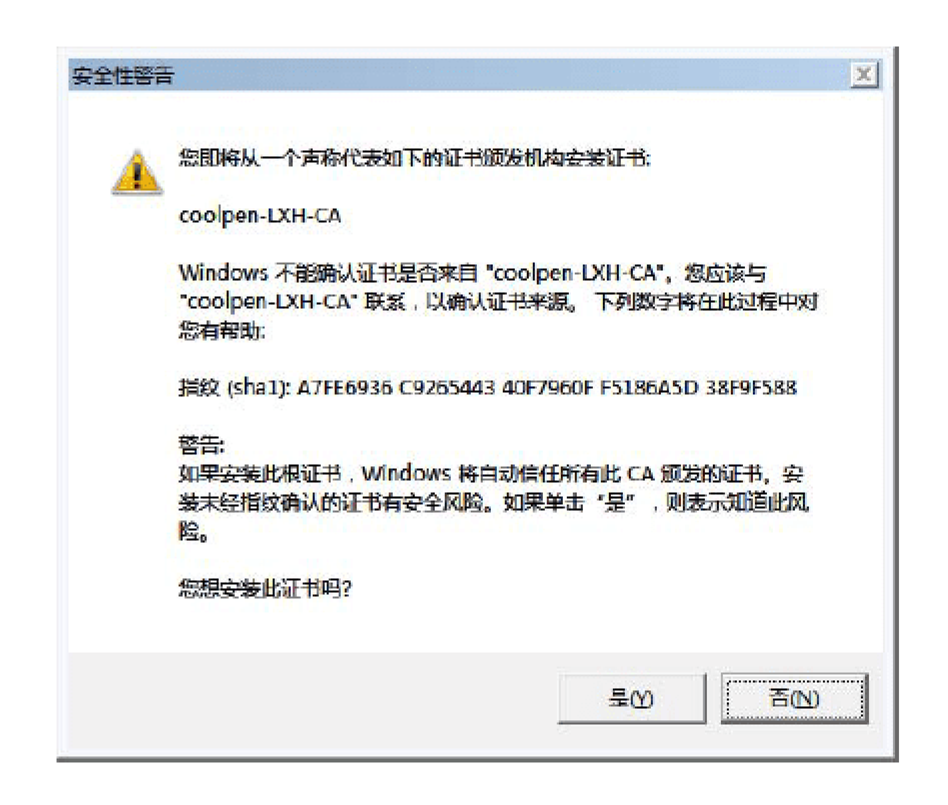


图 10-30　“安全性警告”对话框

⑪　单击“确定”按钮，保存并退出。

(3)　申请证书

①　登录到“Active Directory 证书服务”窗口，在“欢迎使用”窗口中单击“申请证书”超级链接，显示如图 10-32 所示的“申请一个证书”界面。



图 10-31　证书导入成功

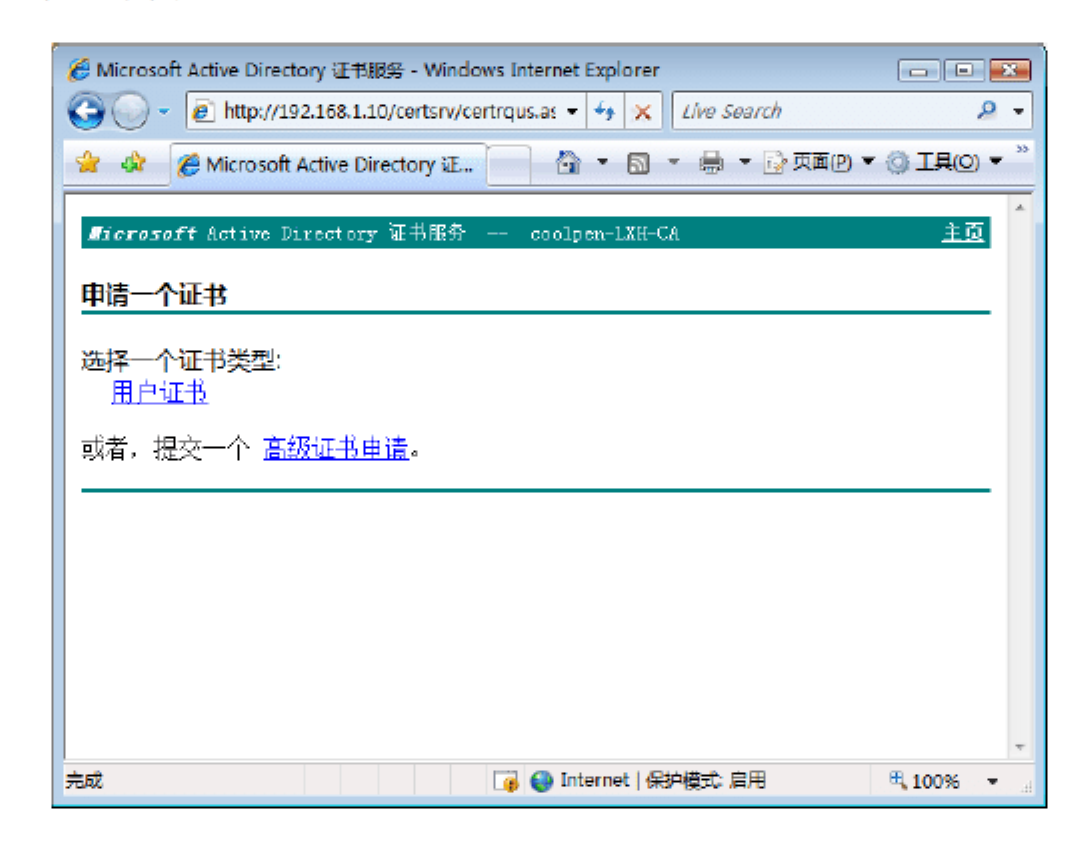


图 10-32　“申请一个证书”界面

②　单击“用户证书”链接，显示如图 10-33 所示的“用户证书 – 识别信息”界面。

③　单击“提交”按钮，即可向证书服务器申请证书，完成后显示如图 10-34 所示的“证书已颁发”界面，提示所申请的证书已颁发。

④　单击“安装此证书”链接，显示如图 10-35 所示的“证书已安装”界面，提示证书已经安装。

2. 使用“证书申请向导”申请证书

要使用“证书申请向导”向企业根 CA 申请证书，客户端计算机必须先加入域，并且使用域用户登录到域。这里以 Windows Vista 为例，介绍如何申请证书。

①　使用域用户账户登录到 Windows Vista 系统。

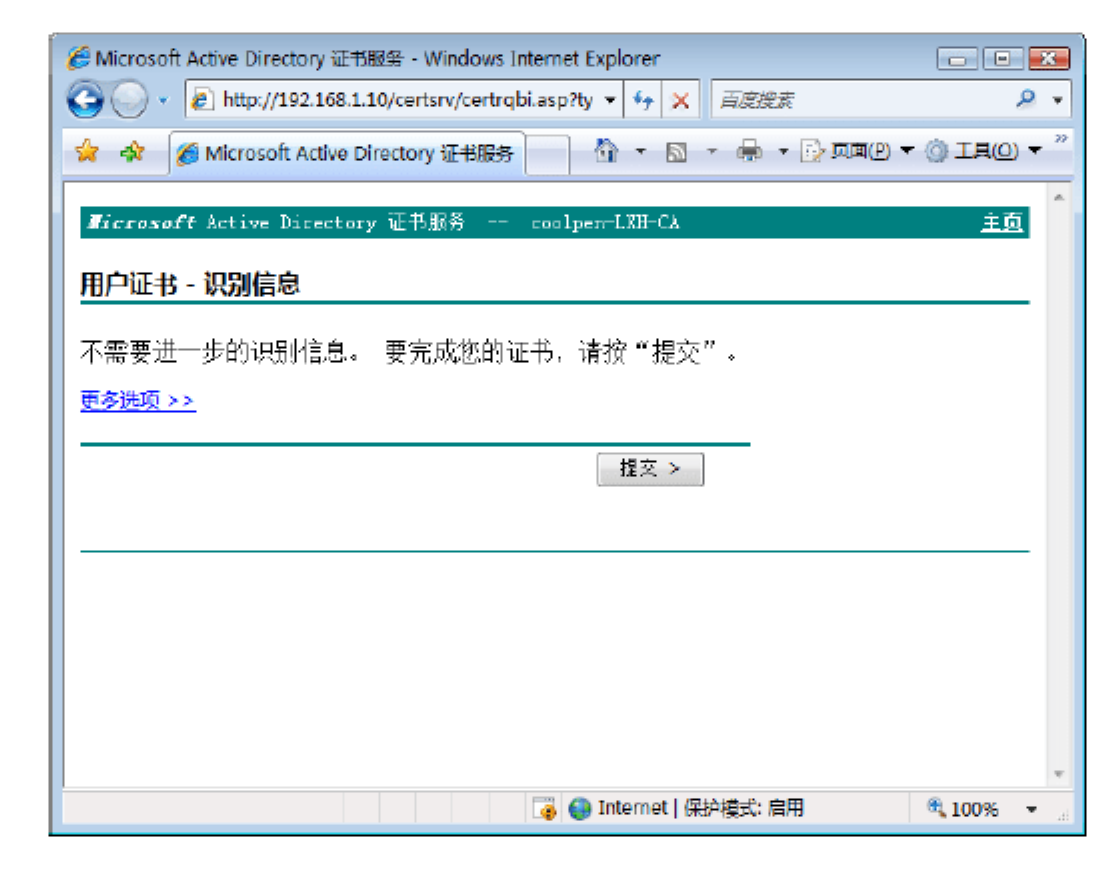


图 10-33　“用户证书 – 识别信息”界面

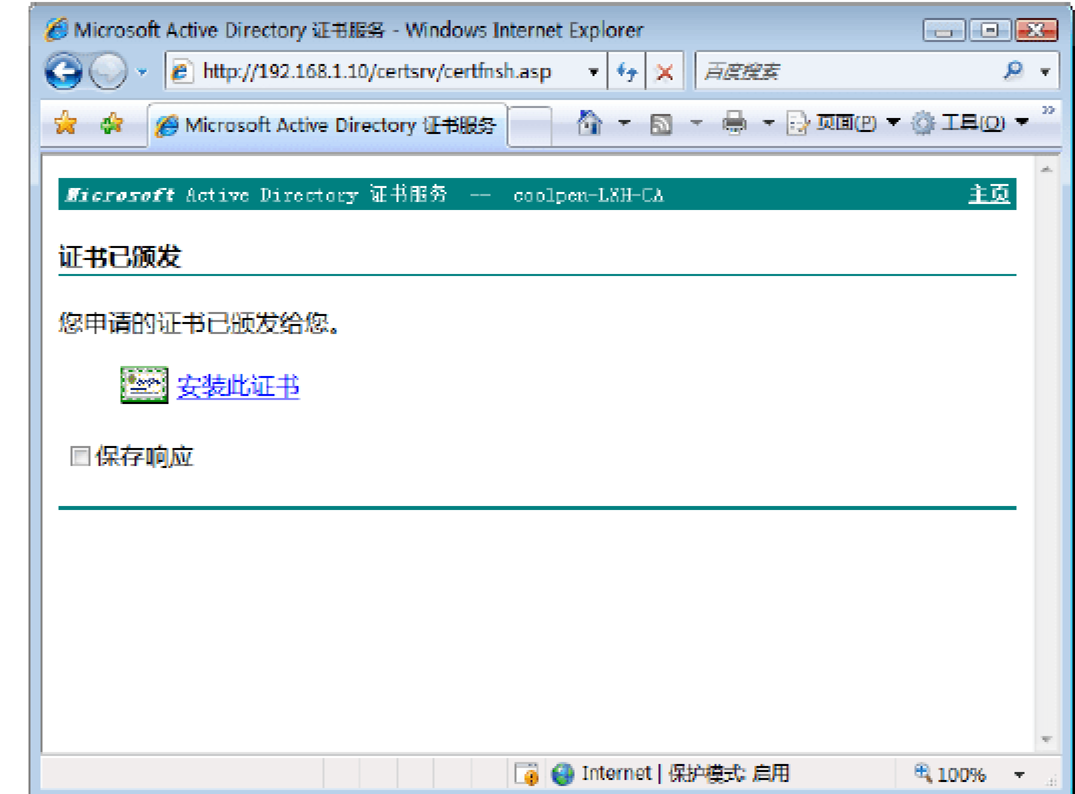


图 10-34　“证书已颁发”界面

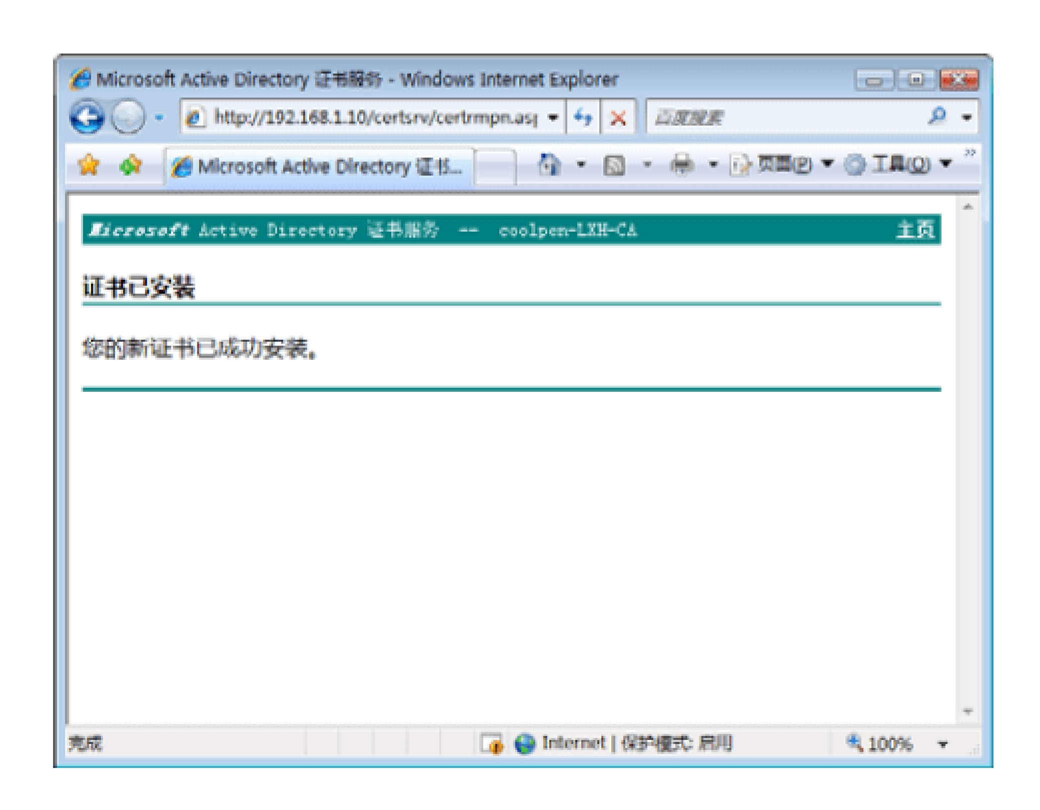


图 10-35　“证书已安装”界面

② 打开“开始”菜单，在“开始搜索”文本框中输入“mmc”命令，按 Enter 键确认，打开“控制台 1”窗口，如图 10-36 所示。

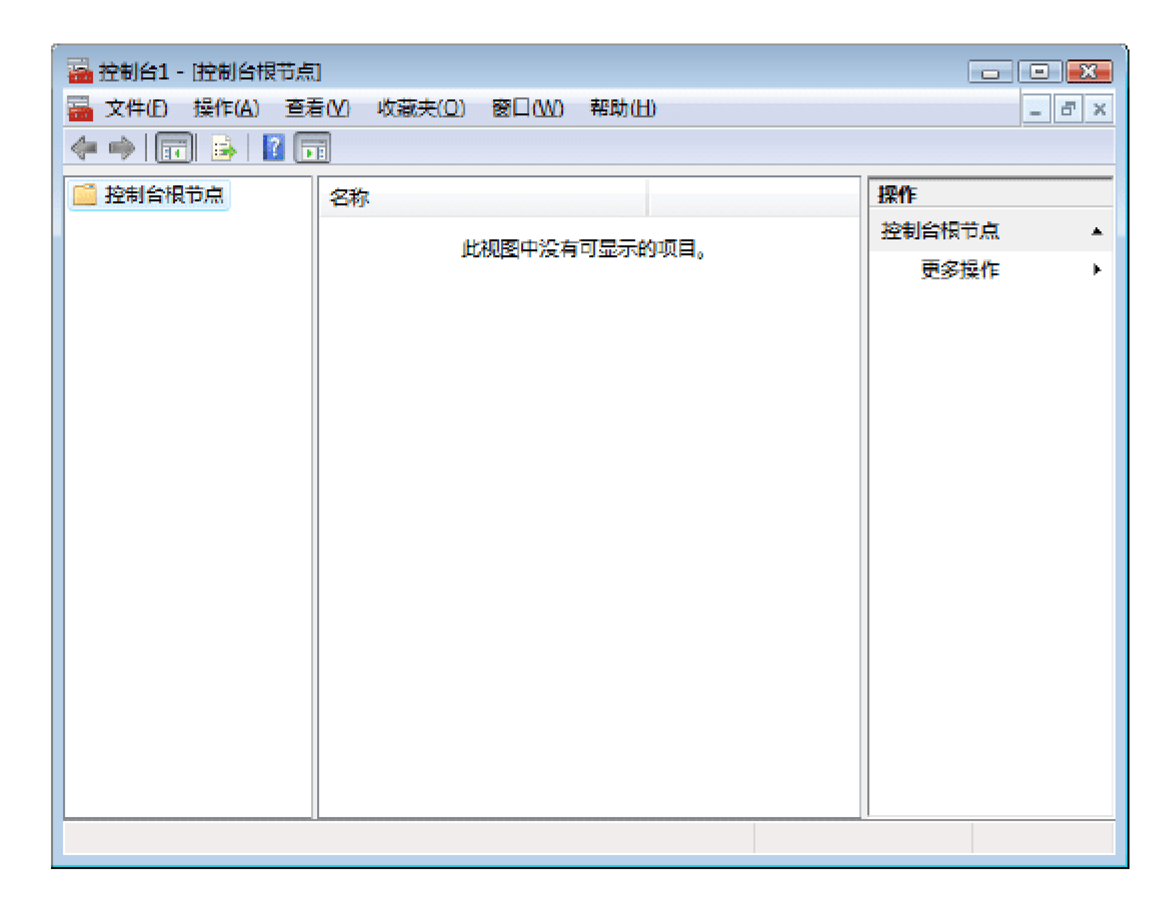


图 10-36　“控制台 1”窗口

③ 单击“文件”菜单中的“添加/删除管理单元”选项，显示“添加或删除管理单元”对话框。在“可用的管理单元”列表框中选择“证书”选项，单击“添加”按钮，添加到右侧“所选管理单元”列表框中，如图 10-37 所示。

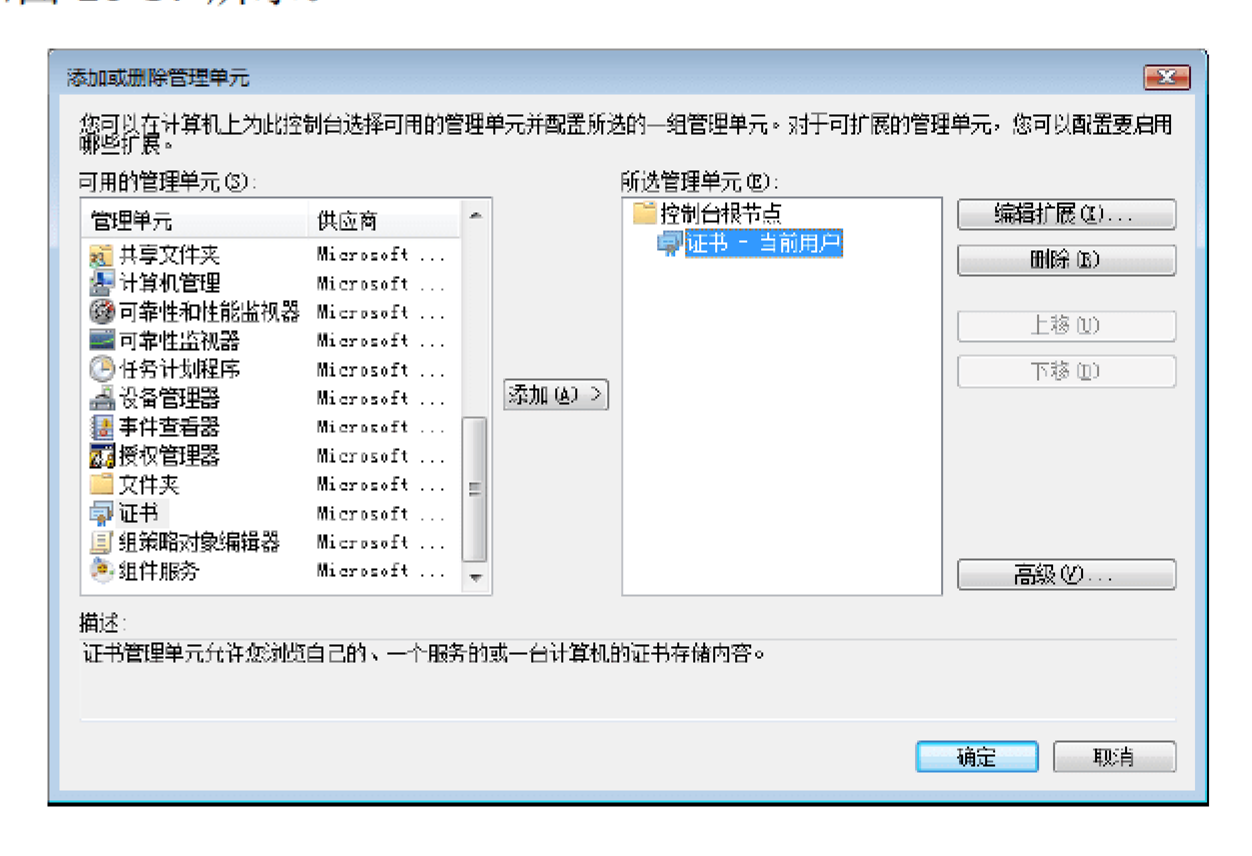


图 10-37　“添加或删除管理单元”对话框

④ 单击“确定”按钮，将证书管理单元添加到控制台中，如图 10-38 所示。

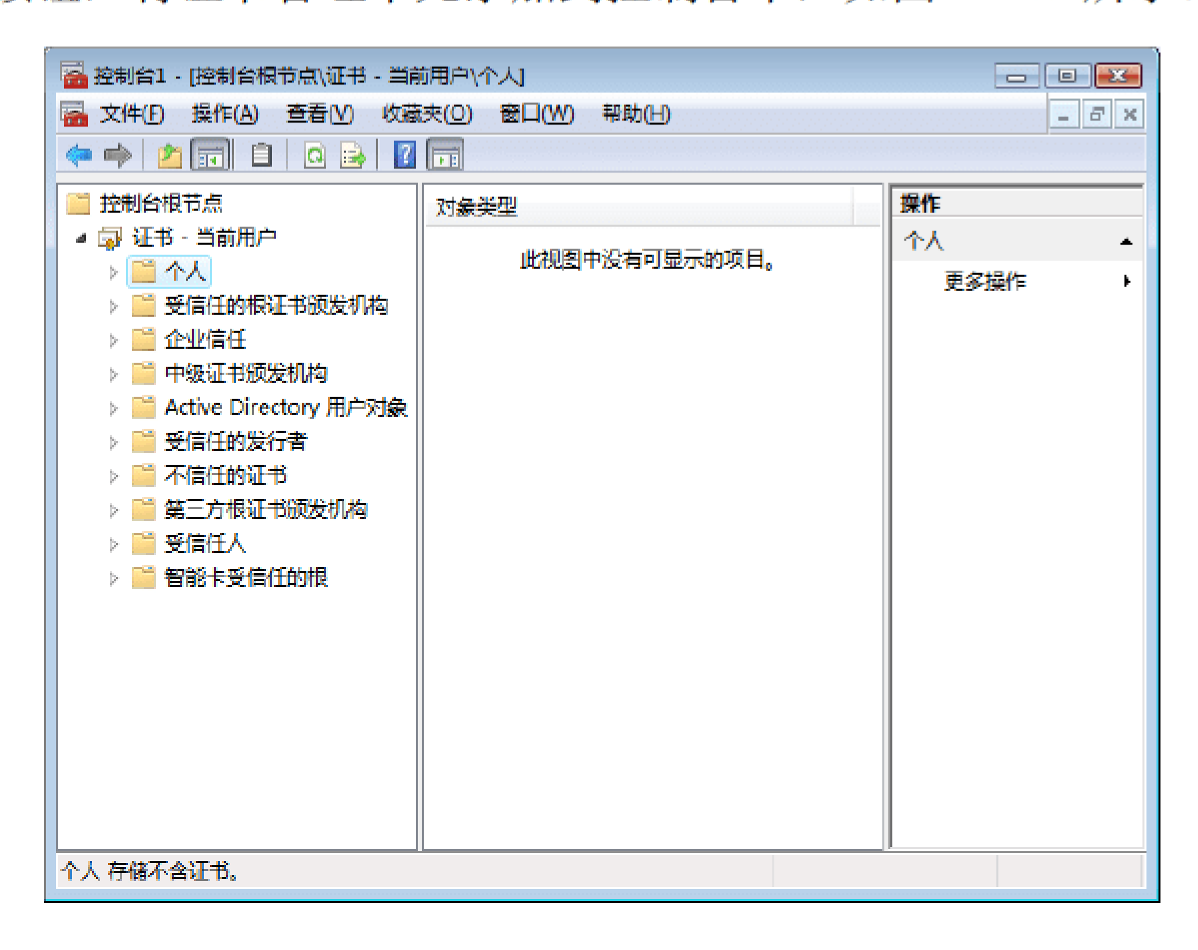


图 10-38　“证书”控制台

⑤ 展开“证书 – 当前用户”，选择“个人”右击，选择快捷菜单中的“所有任务”→“申请新证书”命令，启动“证书注册”向导，显示如图 10-39 所示的对话框。

⑥ 单击“下一步”按钮，显示如图 10-40 所示的“申请证书”界面，在列表框中选择欲申请的证书类型，单击“详细信息”按钮，可以查看该证书的详细信息。默认情况下，只列出了可用的证书模板。

⑦ 单击“注册”按钮，系统会向证书服务器申请注册并自动安装，显示如图 10-41 所示的“证书安装结果”界面。

⑧ 单击“完成”按钮关闭证书注册向导，并返回控制台。依次展开“证书 – 当前用户”→“个人”→“证书”，即可看到已注册成功的证书，如图 10-42 所示。

至此，证书注册完成。返回 Windows Server 2008 证书服务器，依次单击“开始”→“管理工具”→

Certification Authority 命令，打开证书颁发机构窗口。选择“颁发的证书”，即可看到所有已颁发的证书，如图 10-43 所示。

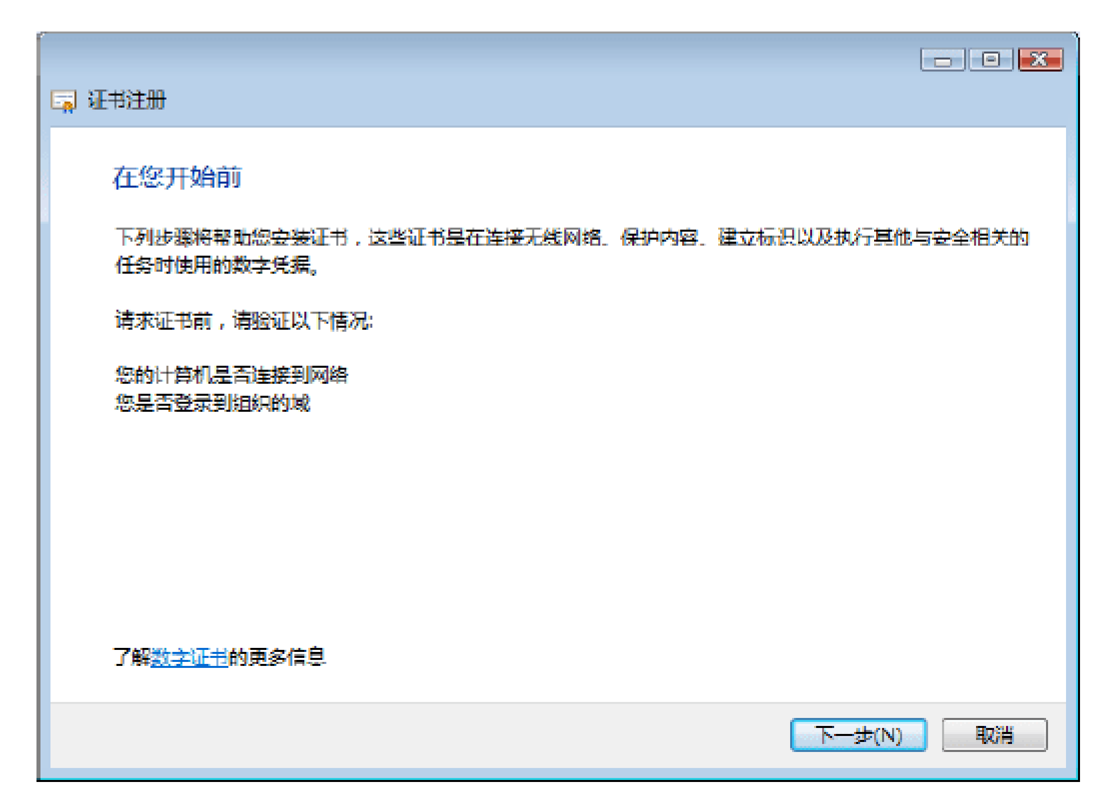


图 10-39　证书注册向导

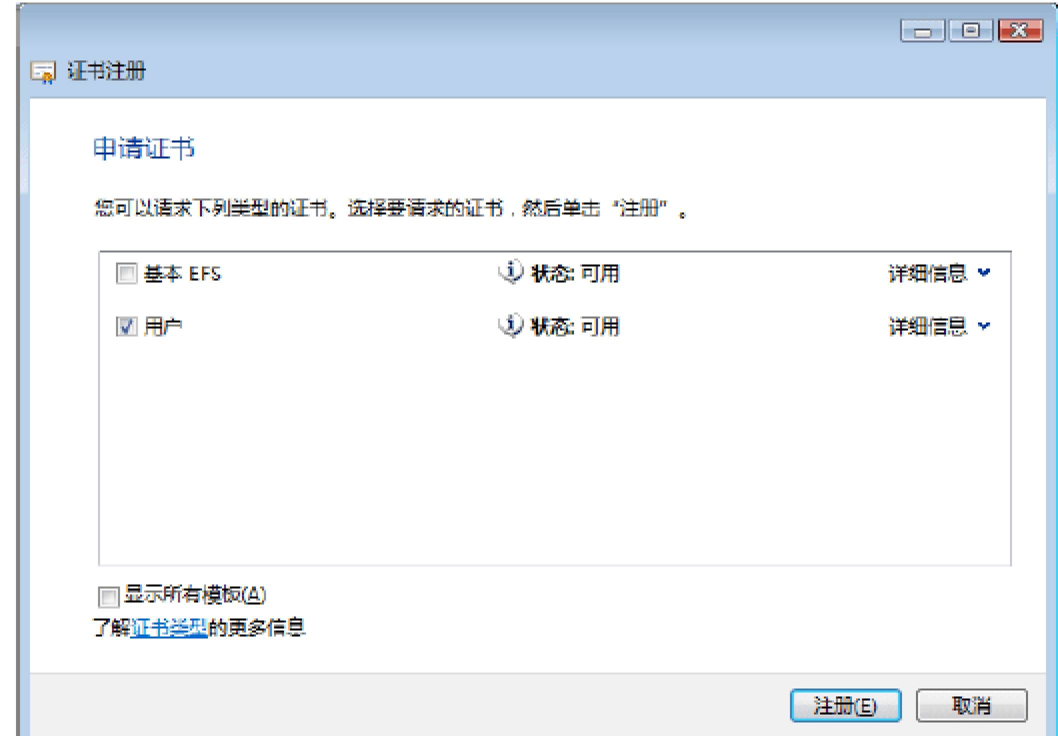


图 10-40　“申请证书”界面

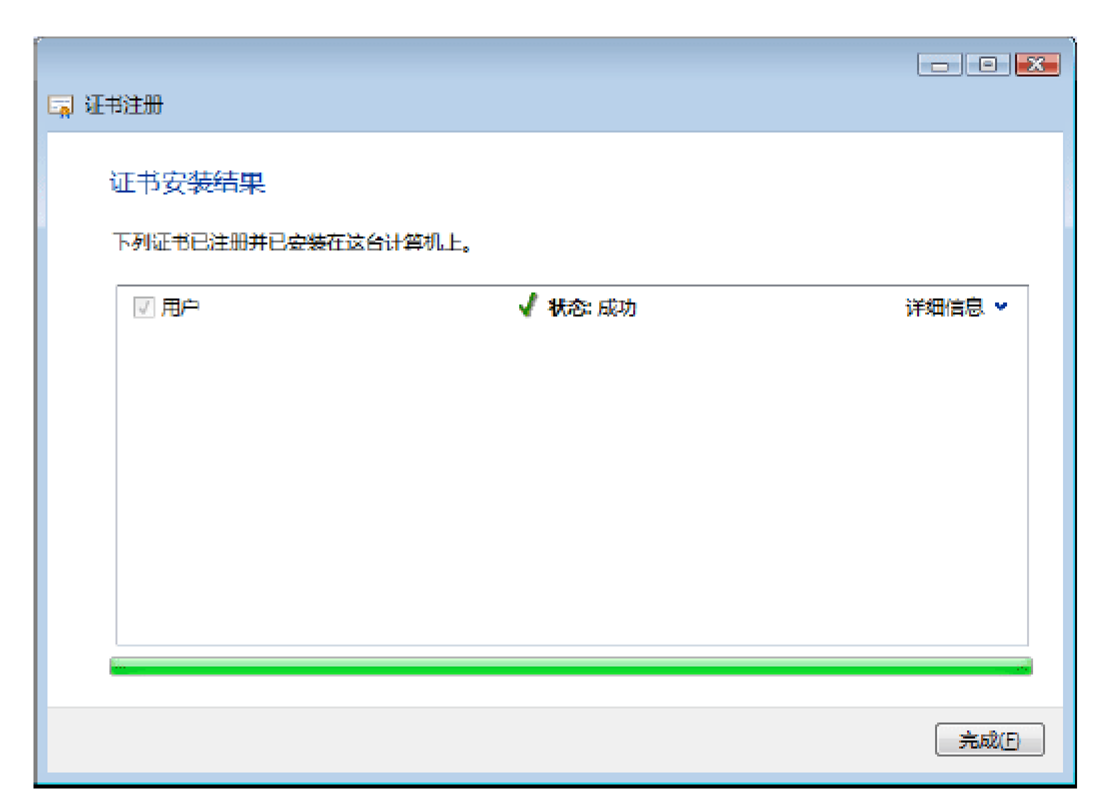


图 10-41　“证书安装结果”界面

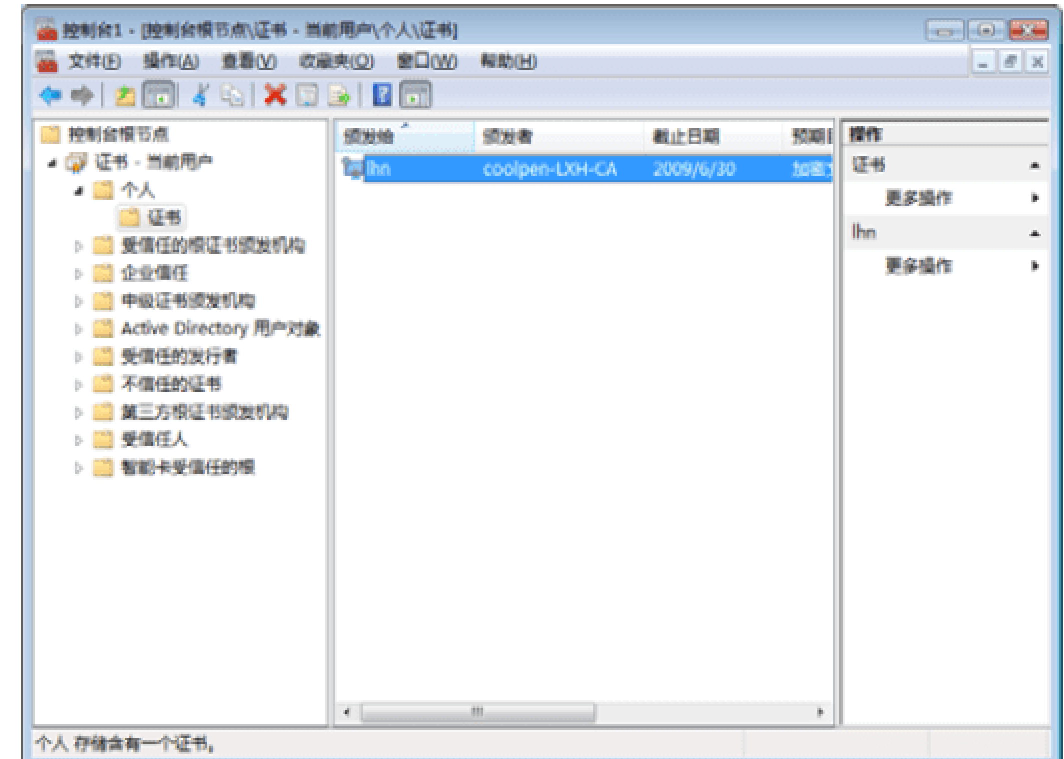


图 10-42　注册成功的证书

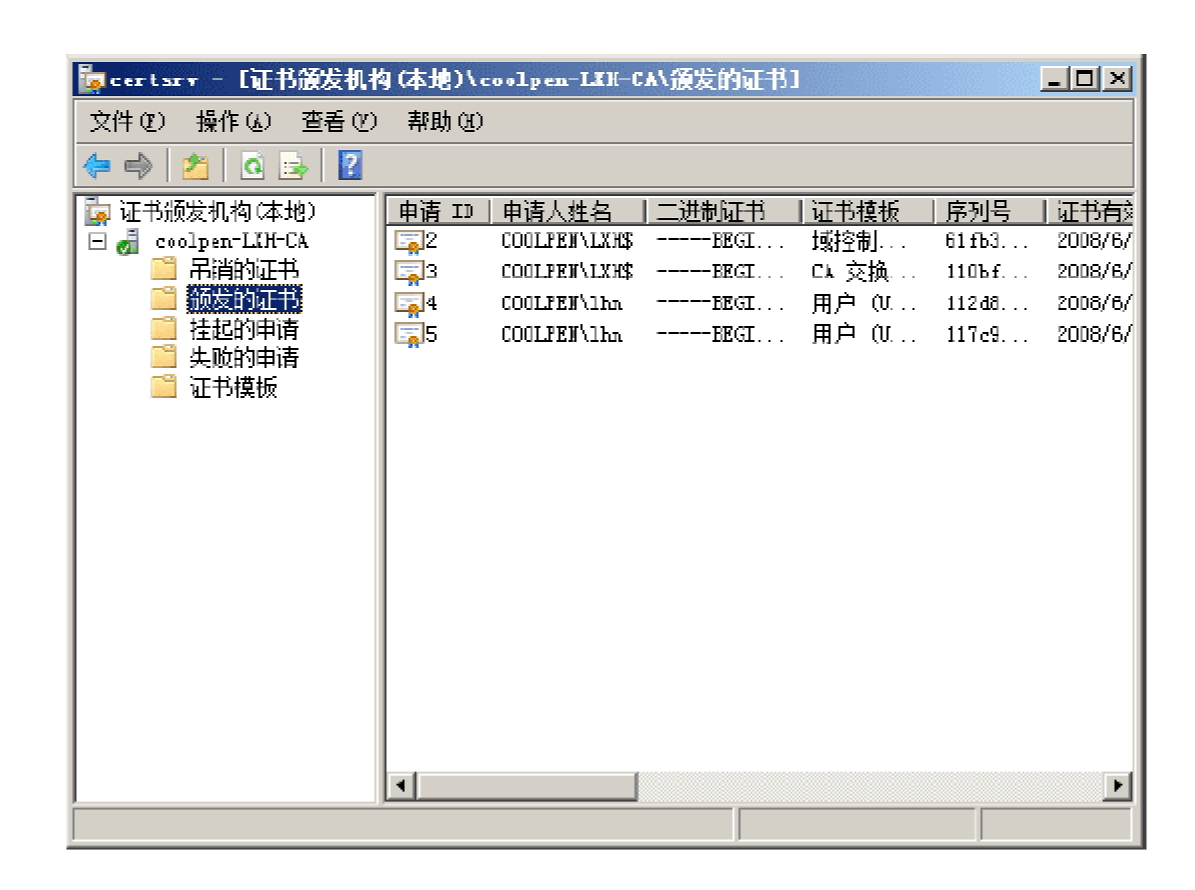


图 10-43　已颁发的证书

10.2.2　独立证书服务的使用

独立证书服务器由于没有加入域，因此，不能使用“证书申请向导”来申请证书，只能以 Web 方式向证书服务器申请证书。为了证书服务的安全，当用户申请证书后并不会立即安装，必须由管理员颁发后才能使用。

1. 申请证书

在向服务器申请证书时，必须先做好如下准备工作。

- 在 IE 浏览器的安全设置中，将“对未标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本(不安全)”和“允许运行以前未使用的 ActiveX 控件而不提示”均设置为“启用(不安全)”状态。
- 下载 CA 证书并导入到客户端计算机上的“受信任的证书颁发机构”中，使其信任证书颁发机构。

向独立服务器申请证书的操作步骤如下。

① 在 IE 浏览器中打开申请独立根证书的地址，格式为 http://证书服务器 IP 地址/certsrv，显示如图 10-44 所示的证书服务主页。

② 单击“申请证书”超级链接，显示如图 10-45 所示的“申请一个证书”界面。可以直接申请 Web 浏览器证书或电子邮件证书，也可以提交高级证书申请。

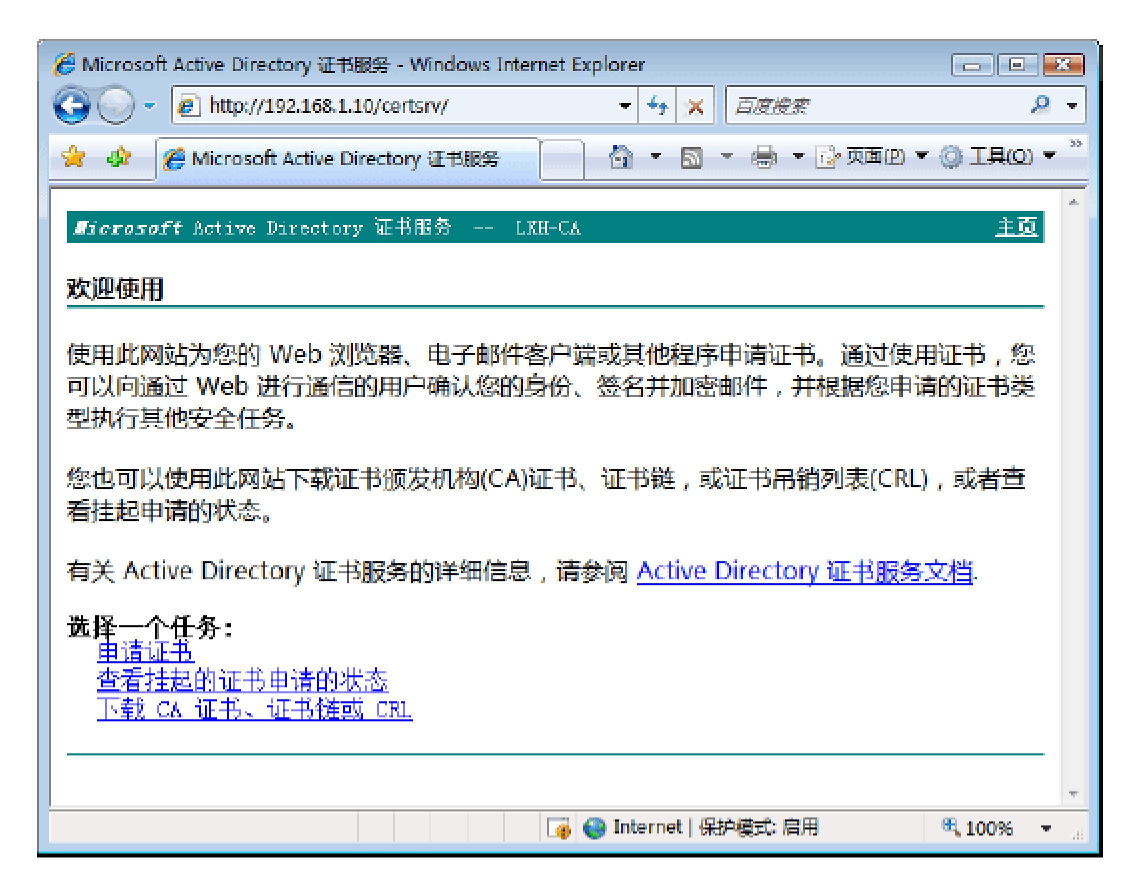


图 10-44　证书服务主页

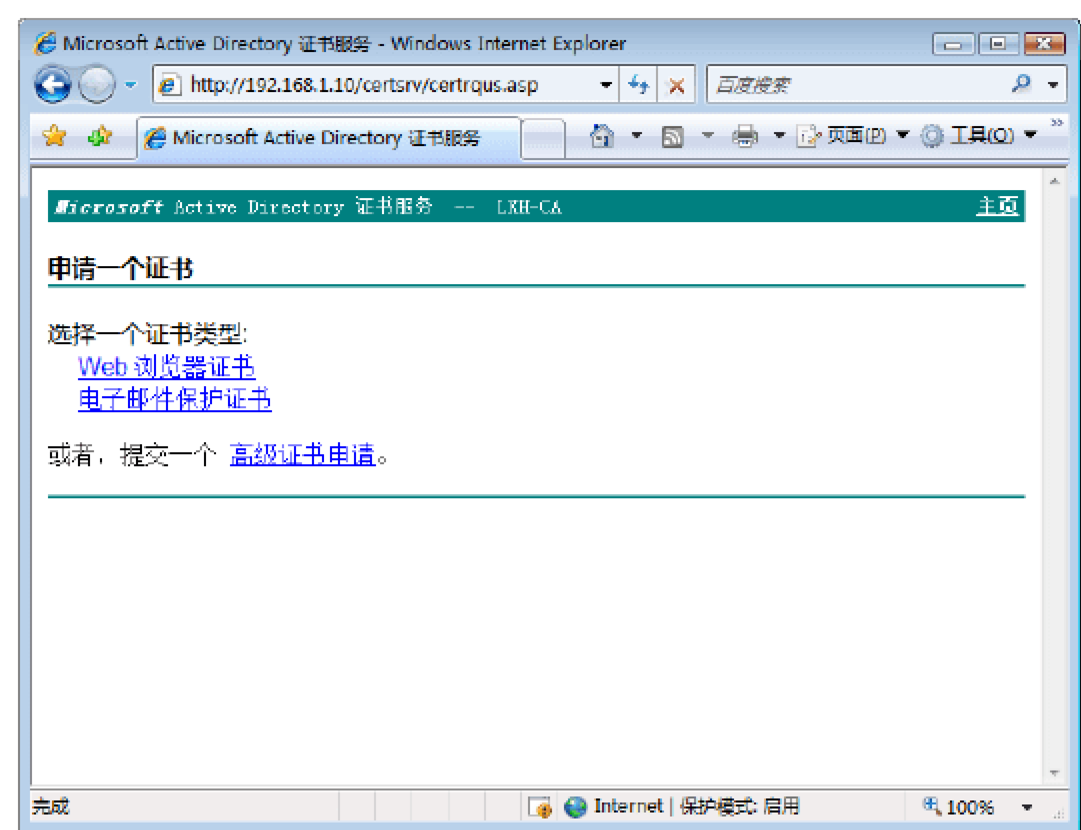
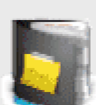


图 10-45　“申请一个证书”界面



提示：如果要申请其他类型的证书，可单击“高级证书申请”链接。同时，还可以选择不同的密钥类型，如图 10-46 所示。

③ 这里以申请电子邮件保护证书为例。单击“电子邮件保护证书”超级链接，显示如图 10-47 所示的“电子邮件保护证书 – 识别信息”界面，在其中输入电子邮件保护证书的识别信息即可。



提示：如果不想使用默认的密钥类型，可以单击“更多选项”链接，显示如图 10-48 所示，在“选择一个加密服务提供程序”下拉列表框中可选择不同的密钥程序。

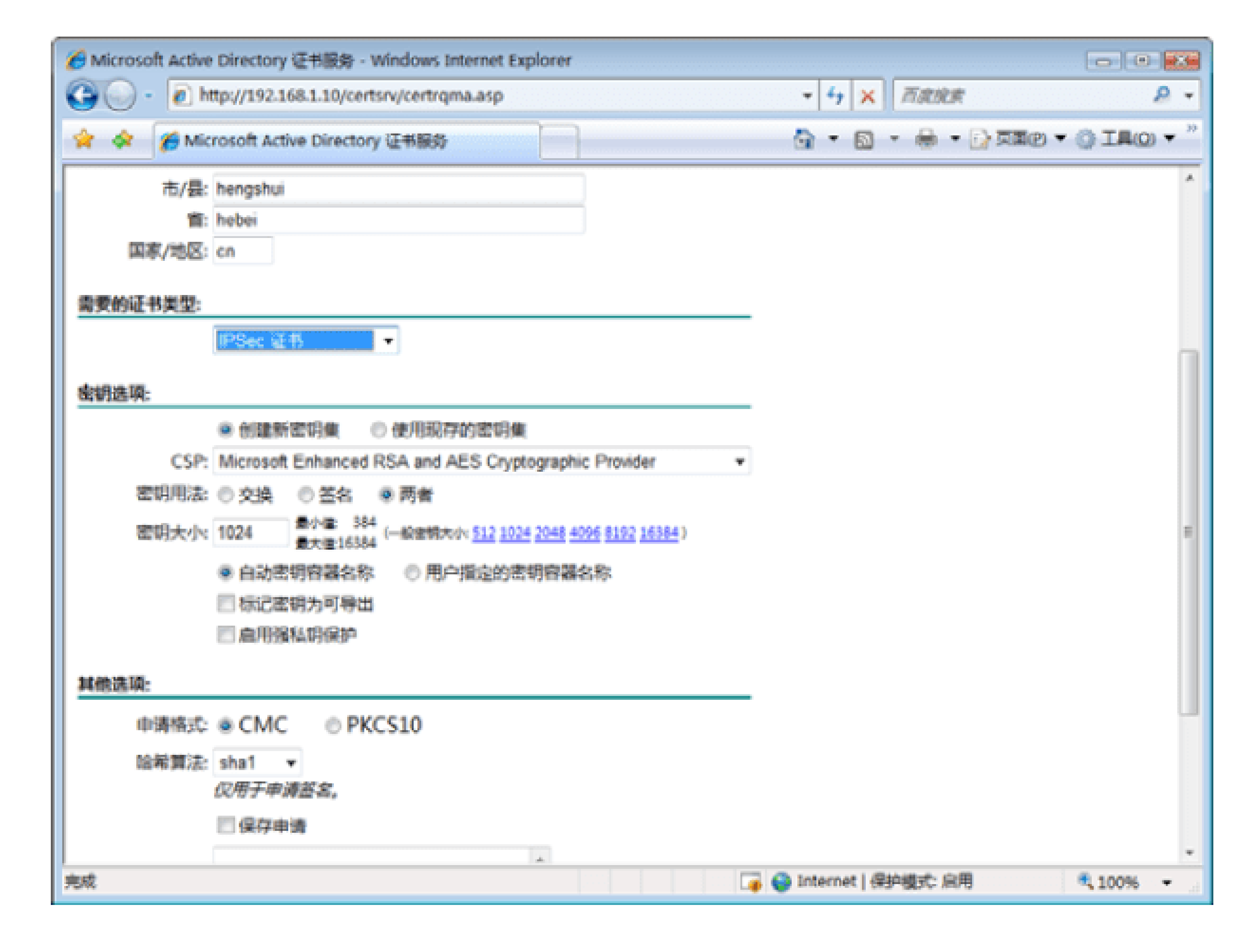


图 10-46　高级证书申请



图 10-47　申请电子邮件证书



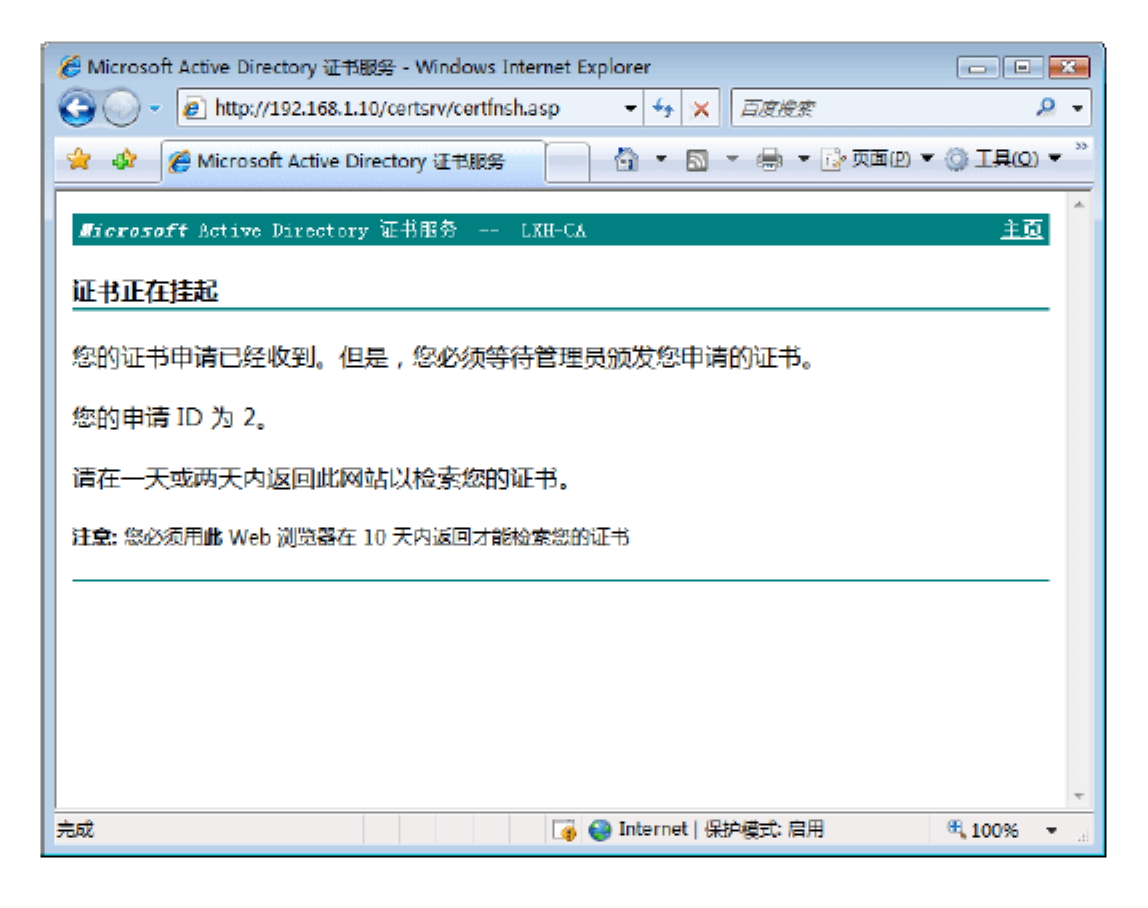
图 10-48　选择不同密钥类型

④ 单击“提交”按钮，开始向证书服务器发送请求，并显示如图 10-49 所示的“证书正在挂起”界面。提示已发出申请，但必须等待管理员来颁发证书。

2. 颁发证书

此时，在 Windows Server 2008 服务器上，需要由管理员查看证书申请，并颁发证书。

① 登录到证书服务器，依次单击“开始”→“管理工具”→Certification Authority 命令，打开 certsrv 窗口。在左侧窗格中选择“挂起的申请”，显示所有提交的证书申请，如图 10-50 所示。



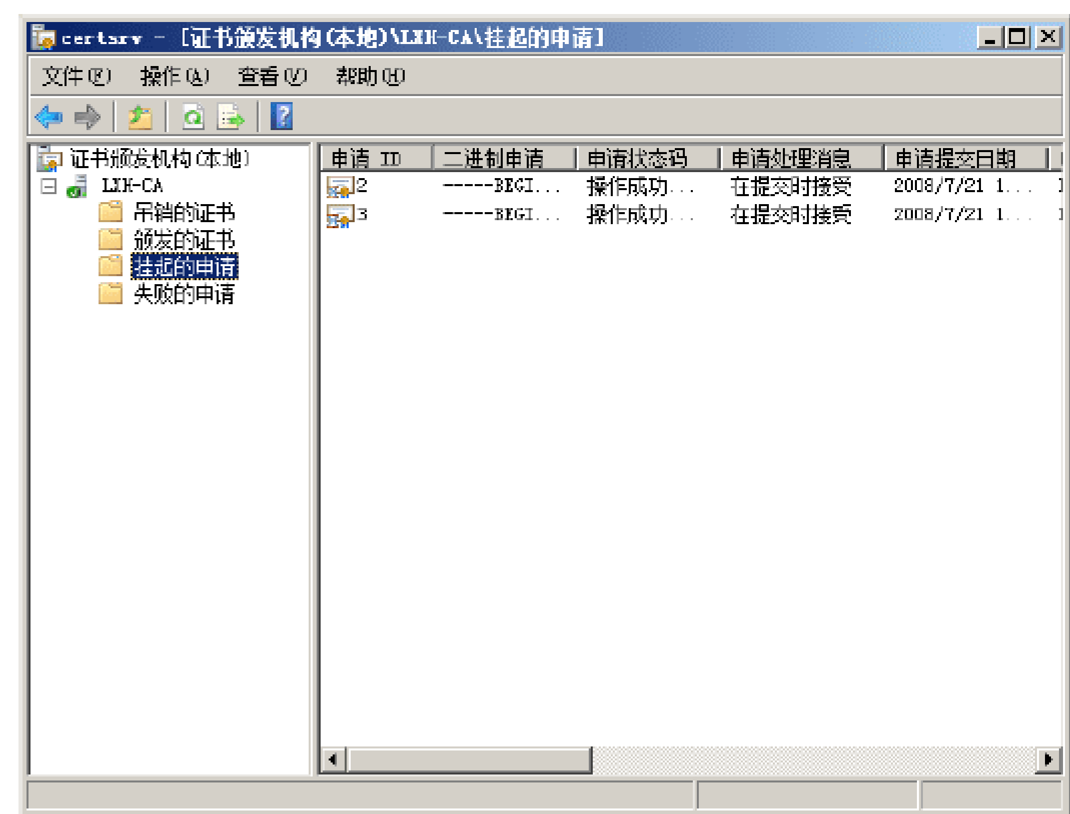


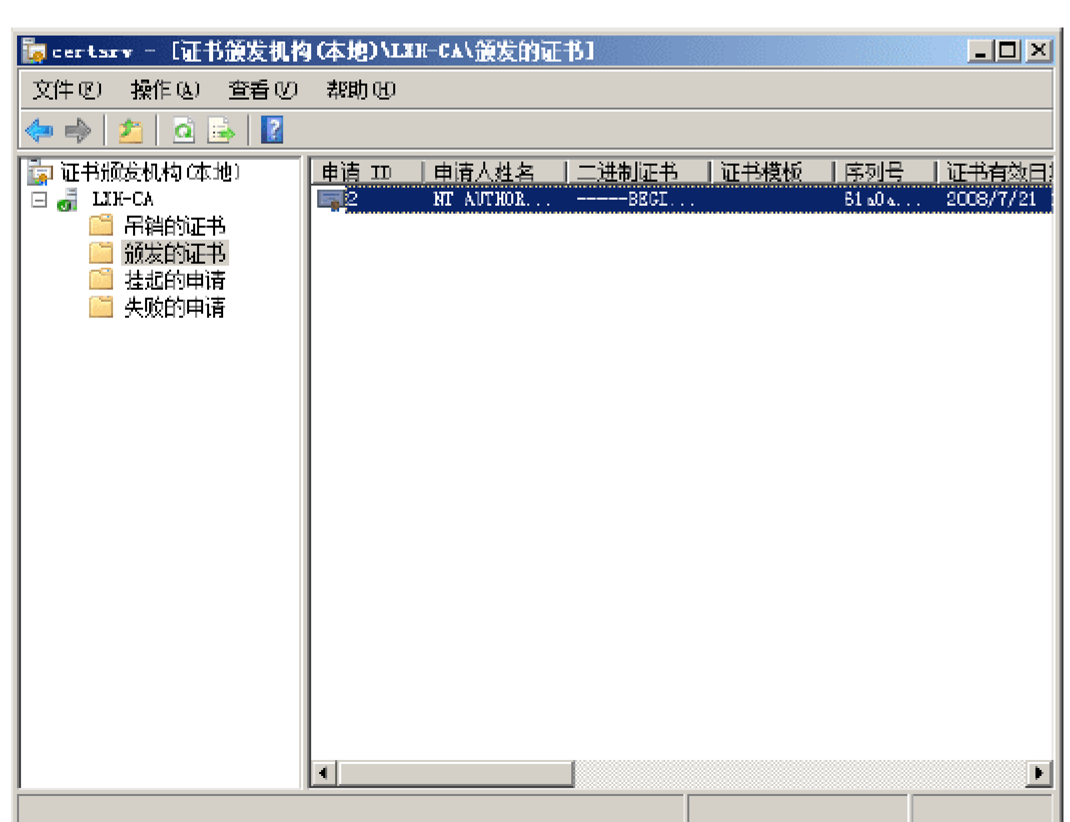
图 10-49 “证书正在挂起”界面　　图 10-50 挂起的申请

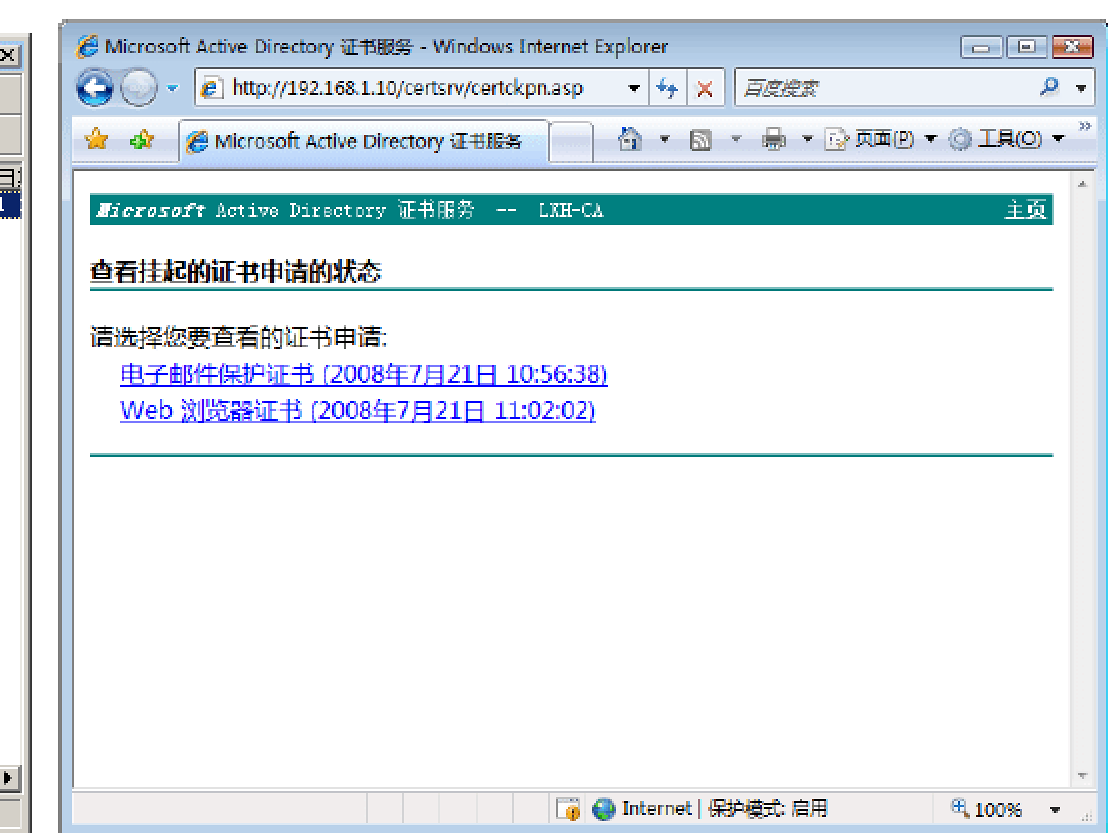
② 选择欲颁发的证书，右击并依次选择快捷菜单中的“所有任务”→“颁发”命令，即可颁发该证书。同时，已颁发的证书将会自动转到“颁发的证书”窗口中，如图 10-51 所示。

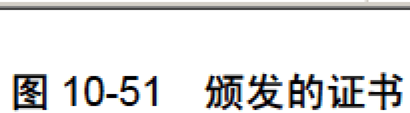
此时，证书颁发完成，在客户端计算机上就可以安装或下载证书了。

3. 客户端 CA 证书的安装

① 在客户端计算机上，重新打开证书服务主页，单击“查看挂起的证书申请的状态”链接，显示如图 10-52 所示的“查看挂起的证书申请的状态”界面，其中列出了曾经申请的证书。






图 10-51 颁发的证书　　图 10-52 “查看挂起的证书申请的状态”界面

② 单击证书名称，例如“电子邮件保护证书”，显示如图 10-53 所示的“证书已颁发”界面，提示该证书已颁发。

③ 单击“安装此证书”链接，显示如图 10-54 所示的“证书已安装”界面，即可将该证书安装在本地计算机上。

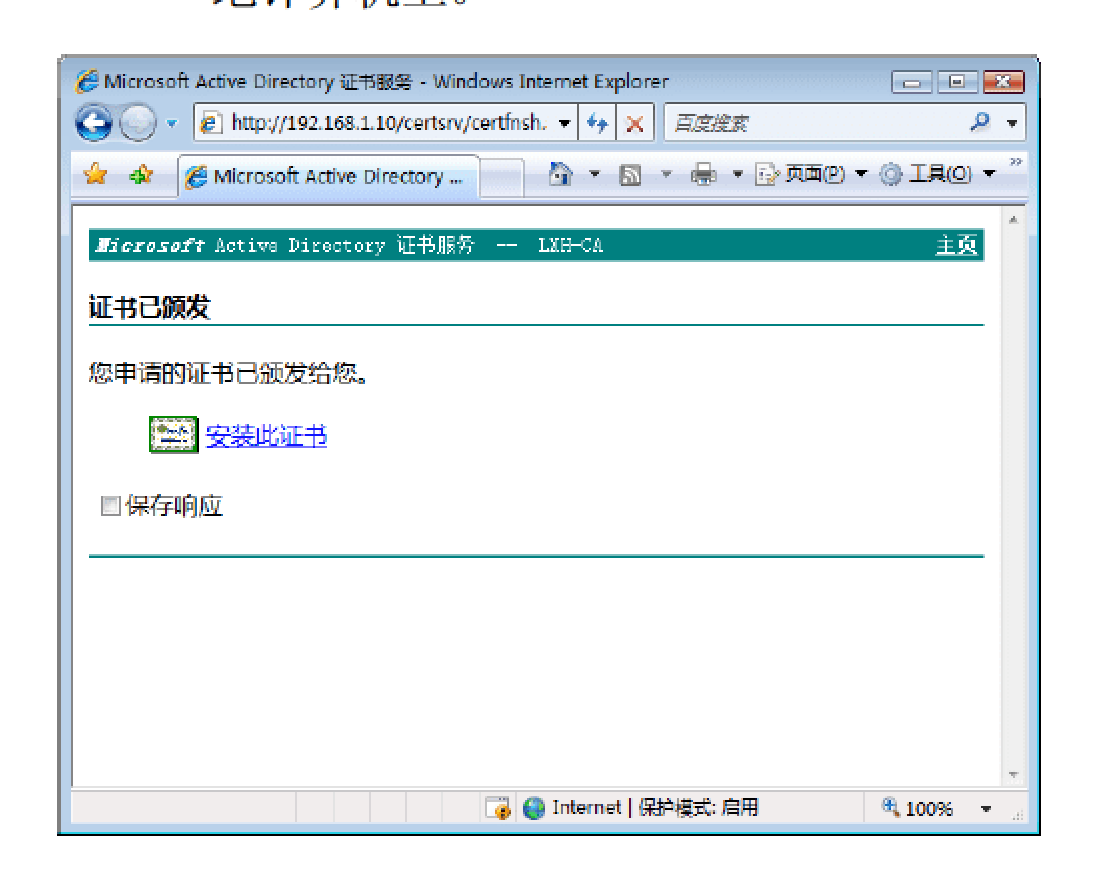




图 10-53 “证书已颁发”界面

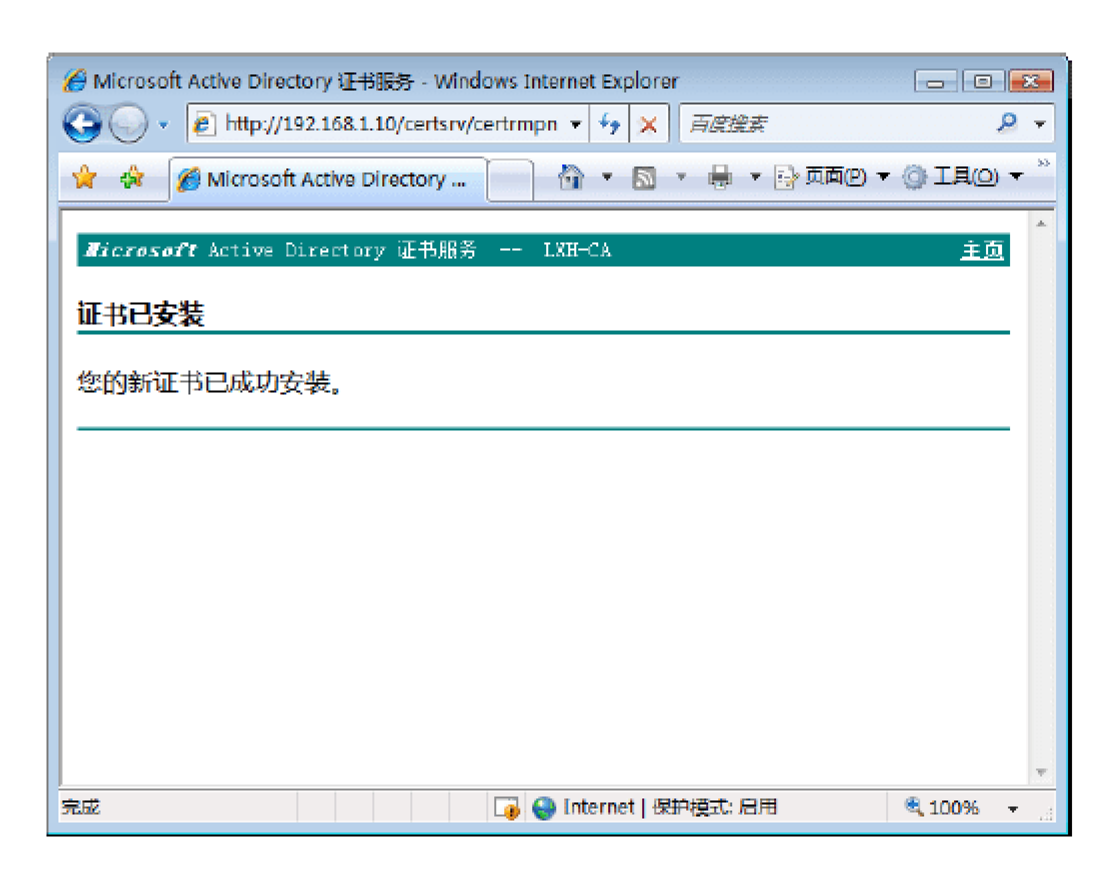


图 10-54 “证书已安装”界面

10.3 CA 证书的管理与应用

在企业中，人员变动是经常发生的事，当员工离开公司或调到其他部门，该员工原来申请的证书将不再使用，此时，网络管理员就应及时吊销其证书。而证书都有一定的有效期限，为了保证在有效期过后仍能继续使用，应及时更新或者续订。

10.3.1 吊销证书

如果某些证书不再使用，需要将其吊销。不过，吊销证书只能在证书服务器上进行，在客户端计算机无法进行吊销证书操作。

① 登录到证书服务器，打开“证书颁发机构”控制台，在“颁发的证书”窗口中选择欲吊销的证书，右击并依次选择快捷菜单中的“所有任务”→“吊销证书”命令，显示如图 10-55 所示的“证书吊销”对话框，在“理由码”下拉列表框中可选择吊销的原因。

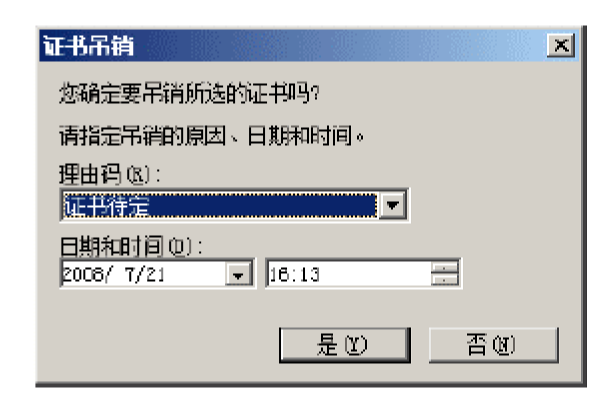


图 10-55 “证书吊销”对话框

② 单击“是”按钮，即可吊销该证书。当证书被吊销以后，将显示在“吊销的证书”窗格中，如

图 10-56 所示。

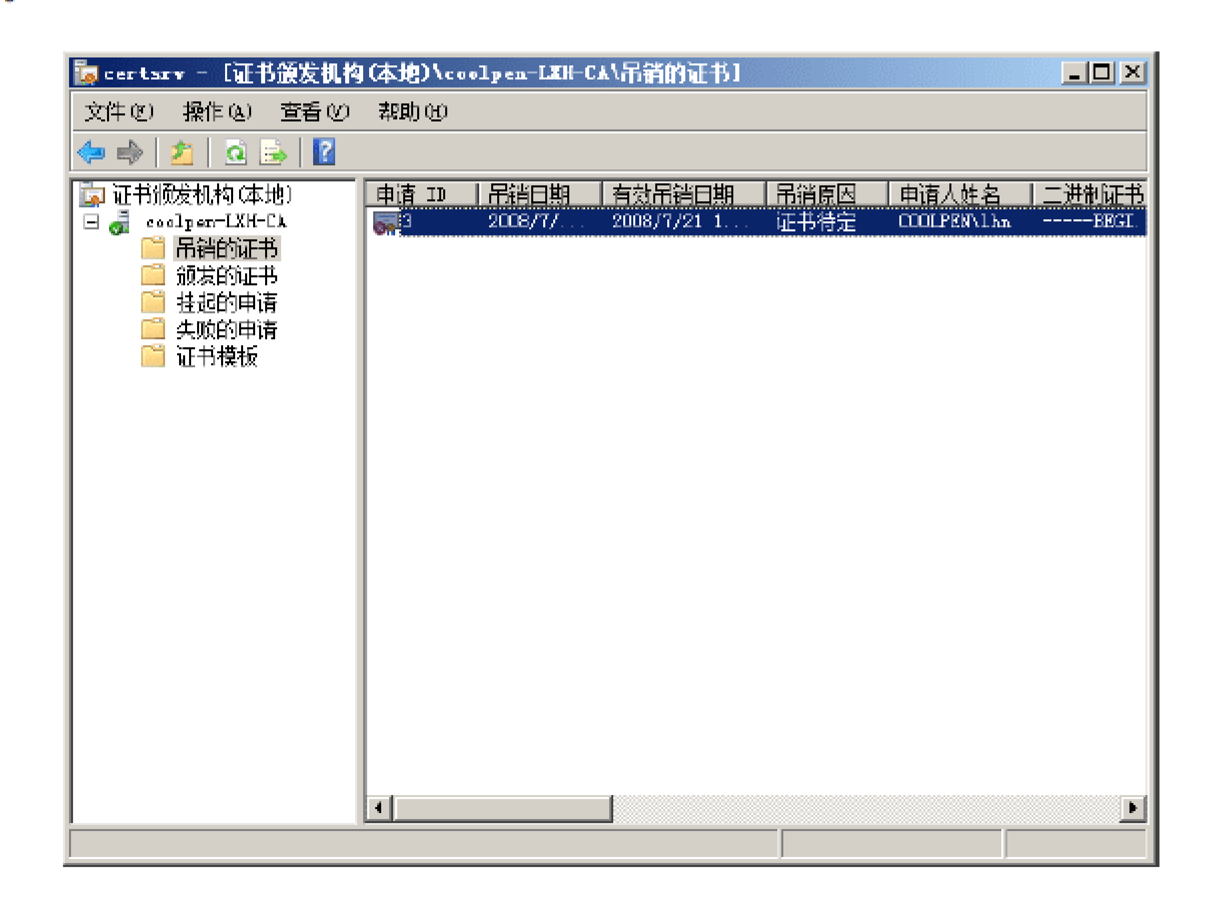


图 10-56　吊销的证书

10.3.2　解除吊销的证书

如果有些已吊销的证书需要继续使用，就可以将这些证书解除吊销。需要注意的是，只有吊销原因为“证书待定”的证书才能解除吊销，因其他原因吊销的证书将不能解除。

在“吊销的证书”窗口中选择欲解除吊销的证书，右击并依次选择快捷菜单中的“所有任务”→“解除吊销证书”命令即可。

如果证书不能被解除吊销，则显示如图 10-57 所示的提示框，提示取消吊销失败。

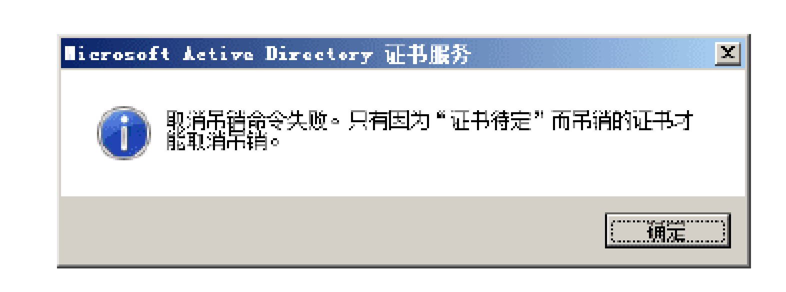


图 10-57　解除吊销失败

10.3.3　证书续订

证书都有一定的有效期限，当有效期过后，证书将会无效。因此，若要继续使用证书，就必须在证书到期前更新或者续订。证书的续订又分为用新密钥续订和使用相同密钥续订。需要注意的是，只有登录到域以后才有权续订证书。

1. 用新密钥续订证书

① 在客户端计算机上运行 MMC 命令打开控制台，添加“证书”管理单元。

② 依次展开“个人”→“证书”，选择欲续订的证书，右击并依次选择快捷菜单中的“所有任务”→“用新密钥续订证书”命令，运行“证书注册”向导，如图 10-58 所示。

③ 单击“下一步”按钮，显示如图 10-59 所示的“申请证书”界面，其中列出了可以请求的证书。单击“详细信息”按钮，可以查看该证书的详细信息。

④ 单击“注册”按钮，开始向证书服务器注册。完成后显示如图 10-60 所示的“证书安装结果”界面，提示注册成功。

⑤ 单击“完成”按钮，证书申请成功。

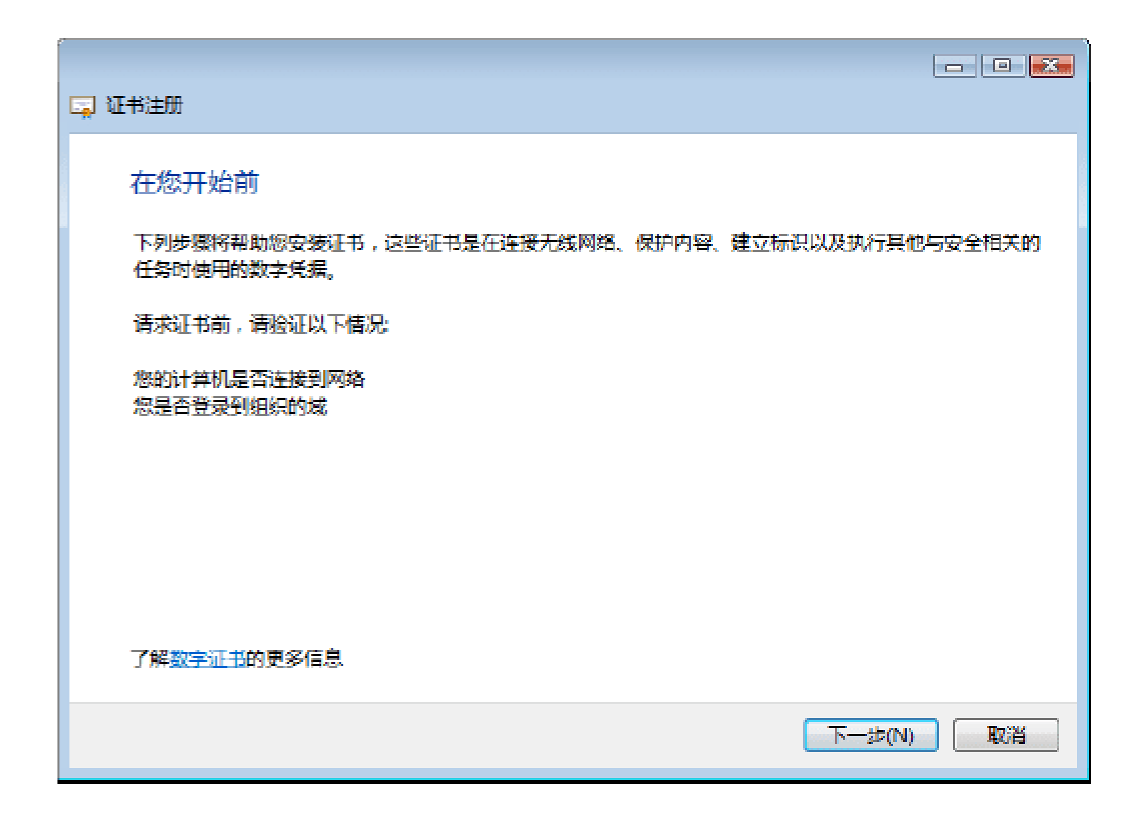


图 10-58　证书注册向导

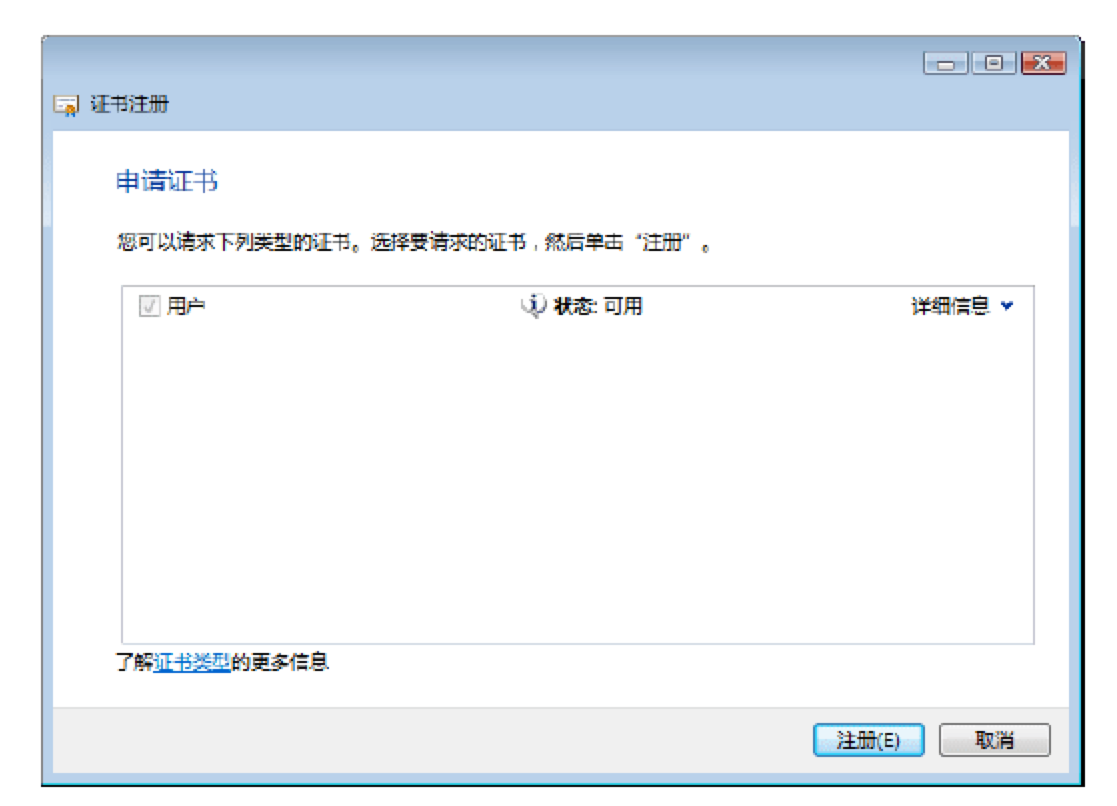


图 10-59　"申请证书"界面

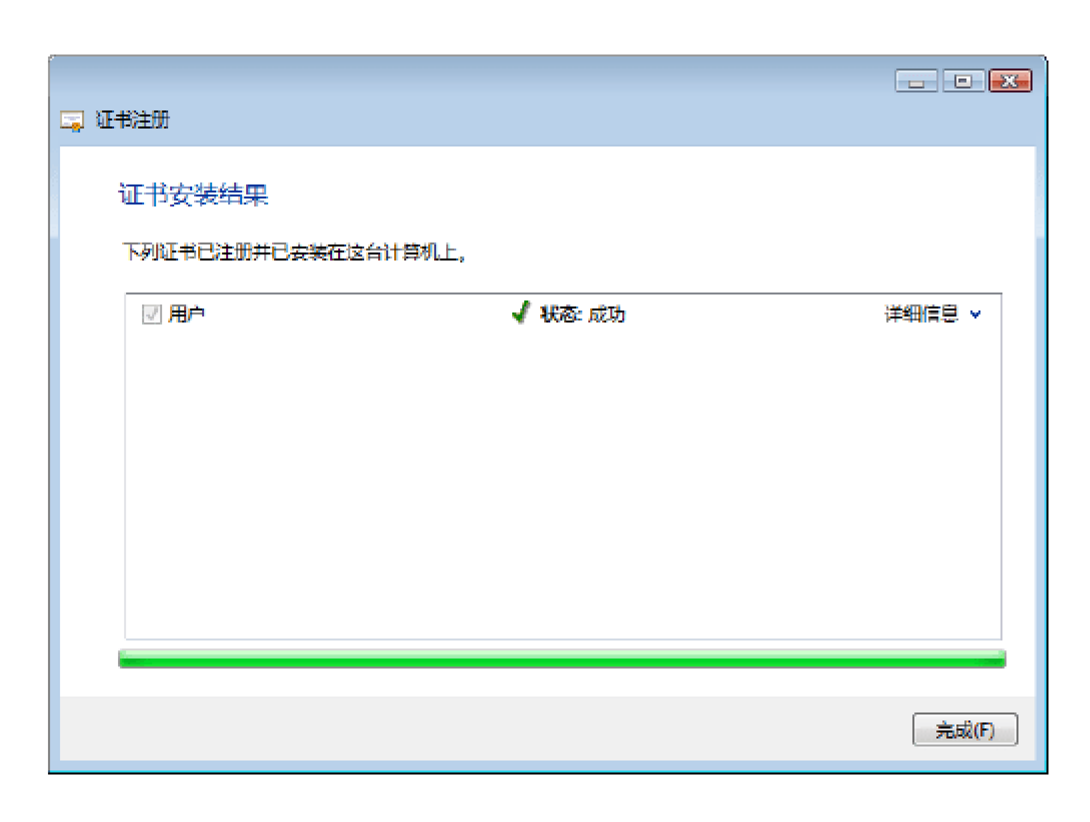


图 10-60　"证书安装结果"界面

2. 用相同密钥续订证书

① 打开"证书"管理单元，选择欲续订的证书，右击并选择快捷菜单中的"所有任务"→"高级操作"→"使用相同密钥续订此证书"命令，运行证书注册向导。

② 单击"下一步"按钮，显示如图 10-61 所示的"申请证书"界面，其中显示了要请求的证书。

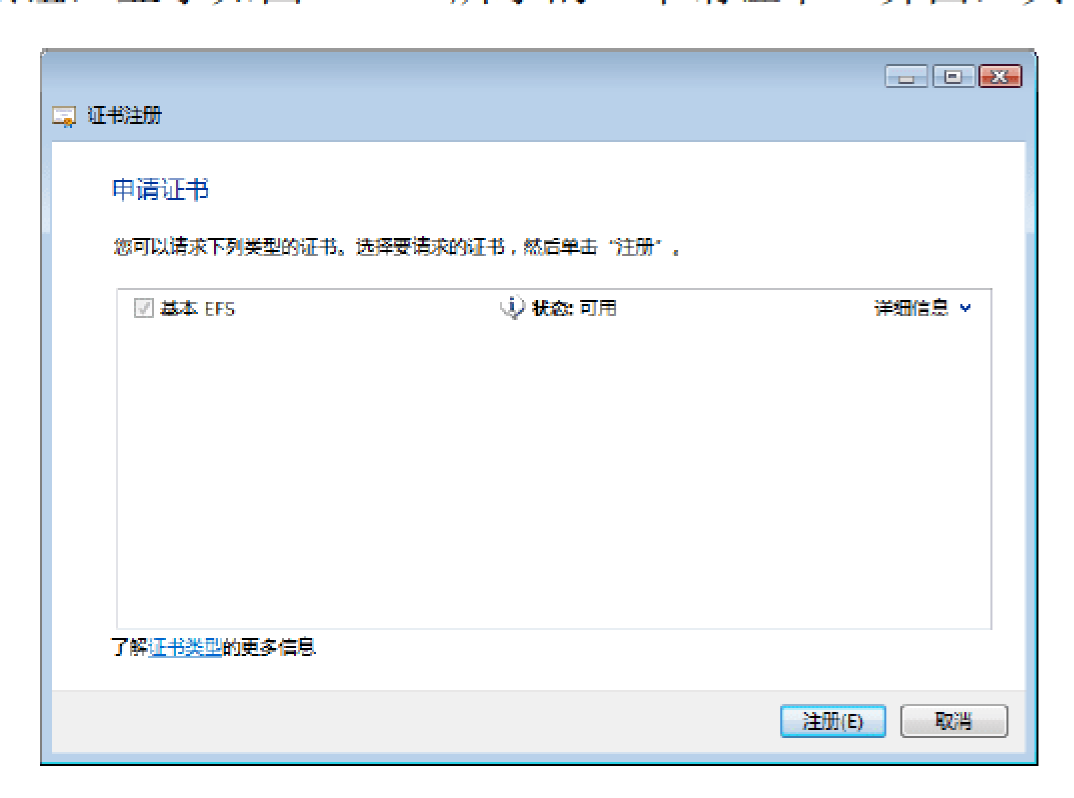


图 10-61　"申请证书"界面

③ 单击“注册”按钮，开始向证书服务器注册，完成后显示如图 10-62 所示的“证书安装结果”界面。

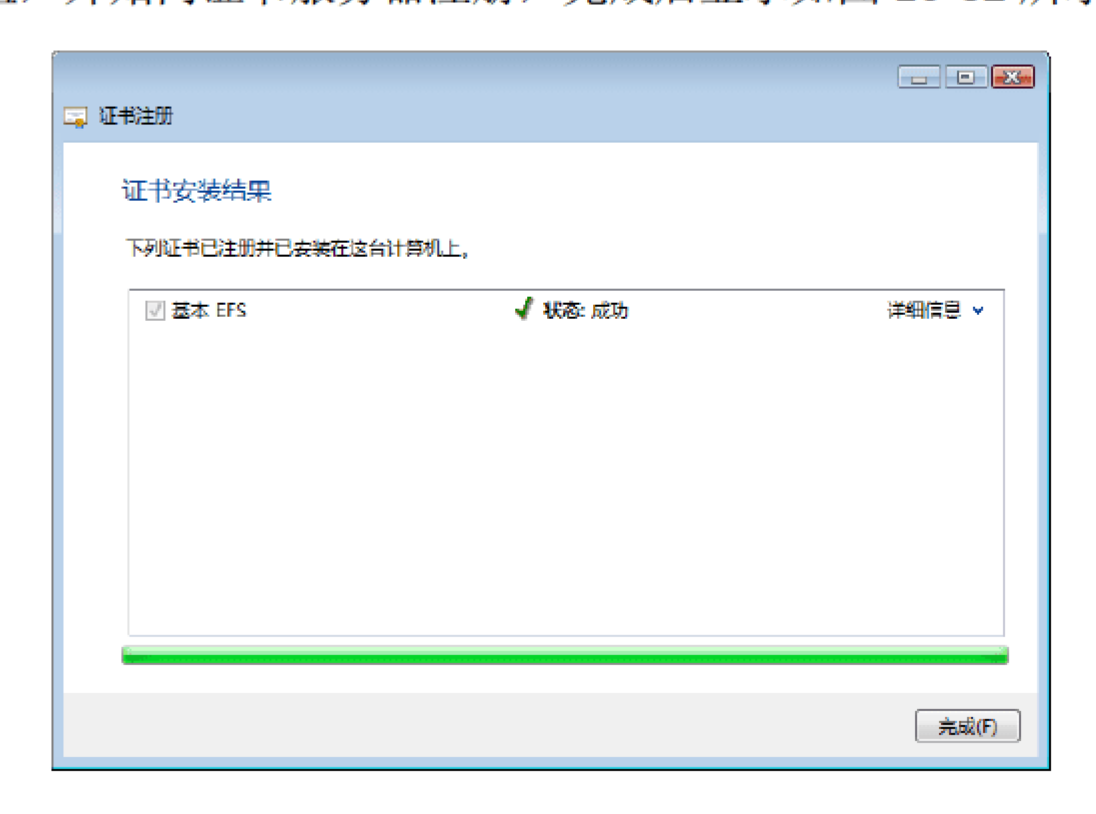


图 10-62 “证书安装结果”界面

④ 单击“完成”按钮，完成证书的续订。

10.3.4 导出与导入证书

为了防止因意外故障或者重新安装系统而造成证书损坏或丢失，用户可以事先将证书导出以进行备份，而当需要还原时，只需将证书导入即可，不必再重新申请。

1. 导出证书

① 在客户端计算机上运行 MMC 命令，打开控制台窗口，添加“证书”管理单元，如图 10-63 所示。

② 展开要备份的证书所在的位置，例如“证书 – 当前用户”→“个人”→“证书”，选择欲导出的证书，右击并依次选择快捷菜单中的“所有任务”→“导出”命令，运行“证书导出向导”，如图 10-64 所示。

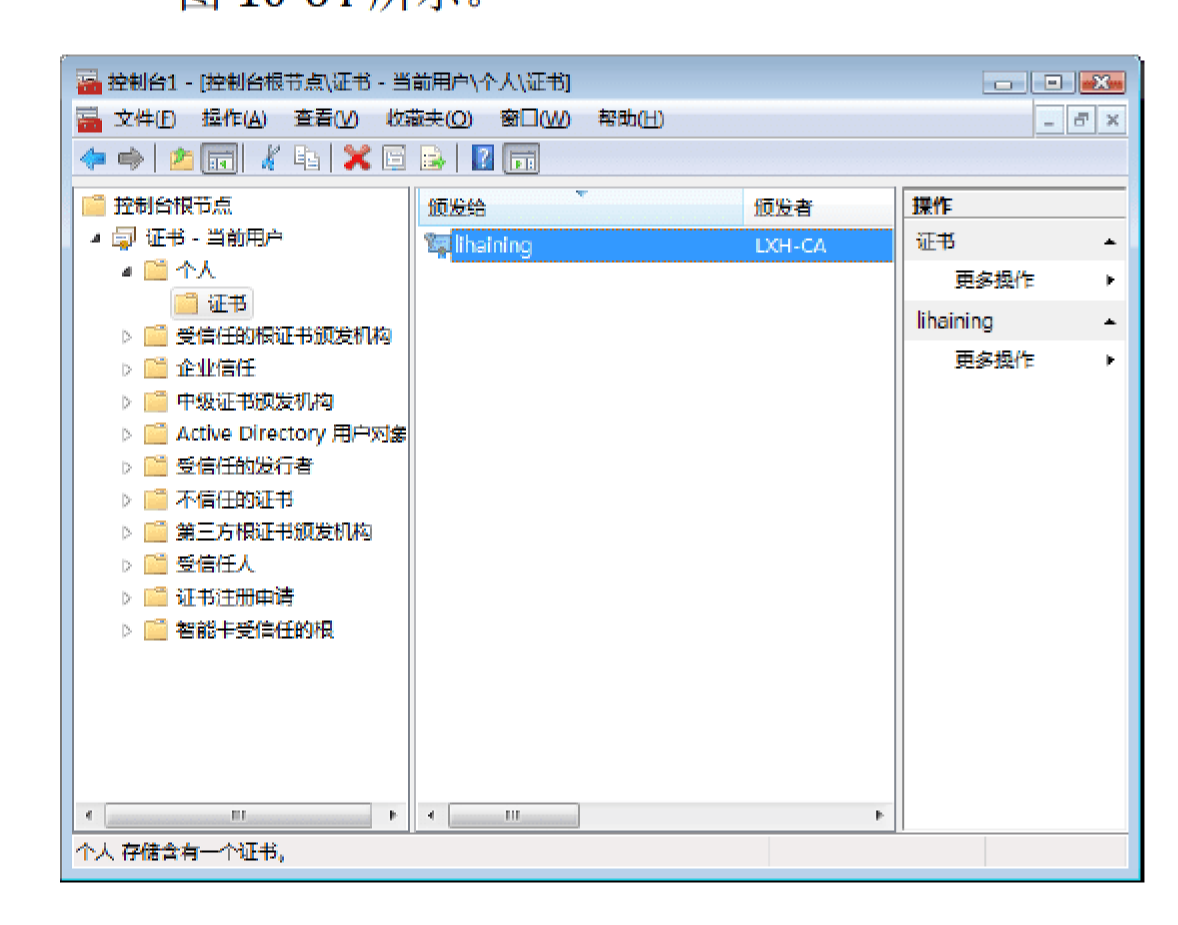


图 10-63 “证书”控制台

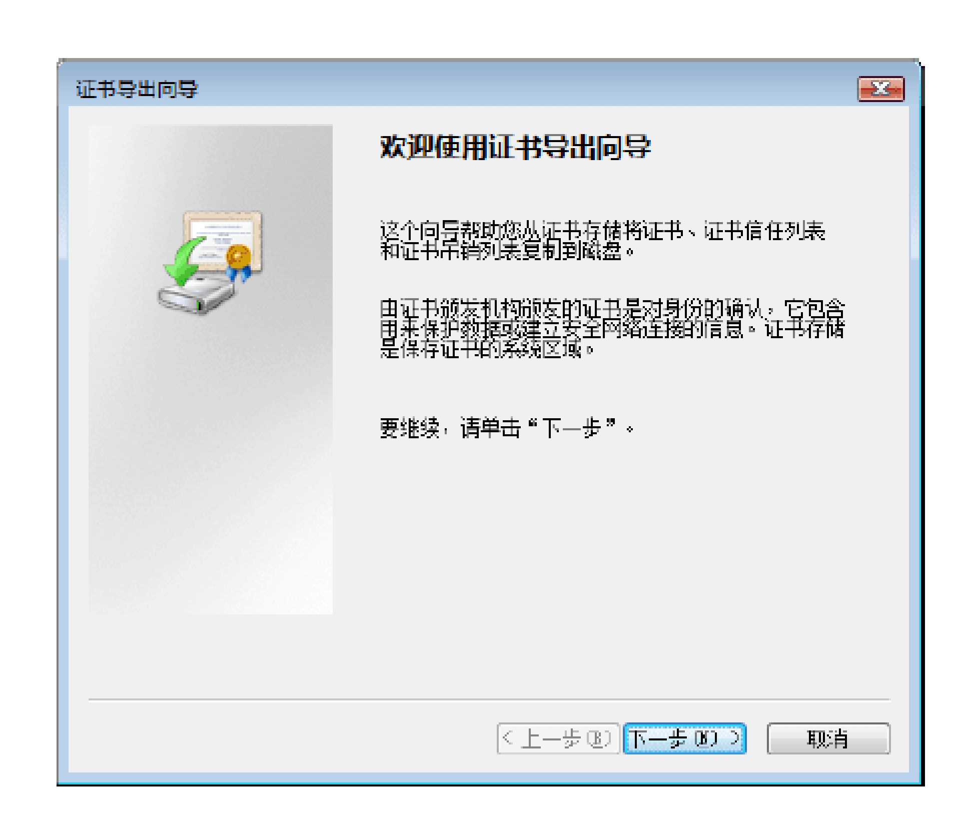


图 10-64 证书导出向导

③ 单击“下一步”按钮，显示如图 10-65 所示的“导出私钥”界面，选择是否要导出私钥。

④ 单击“下一步”按钮，显示如图 10-66 所示的“导出文件格式”界面，选择证书的导出格式。

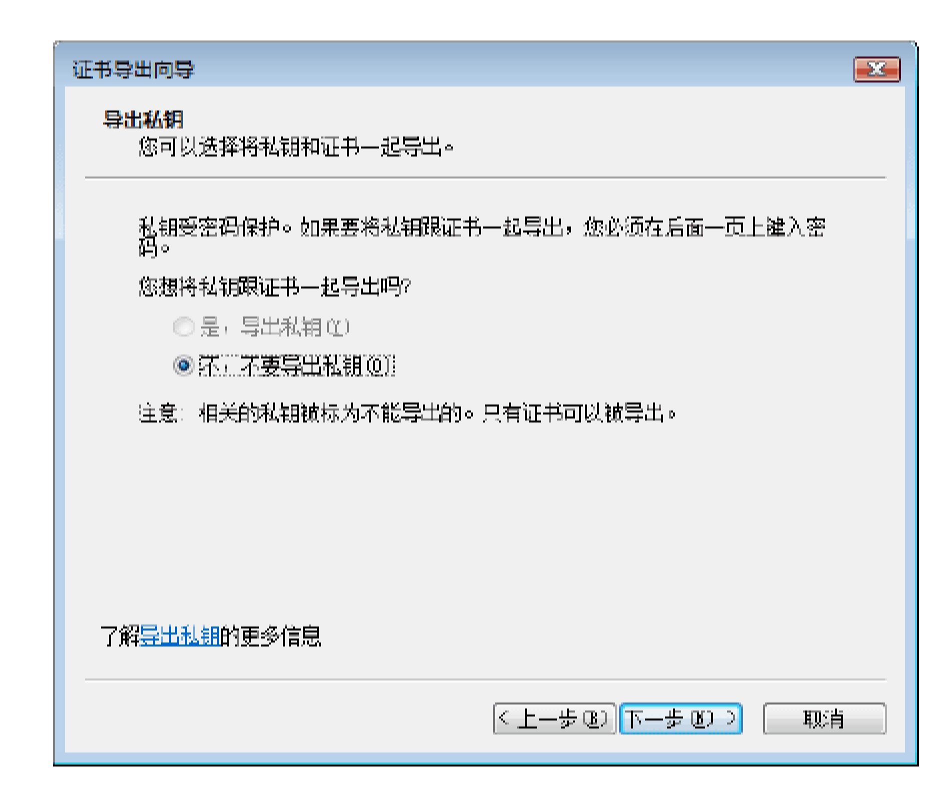


图 10-65 “导出私钥”界面

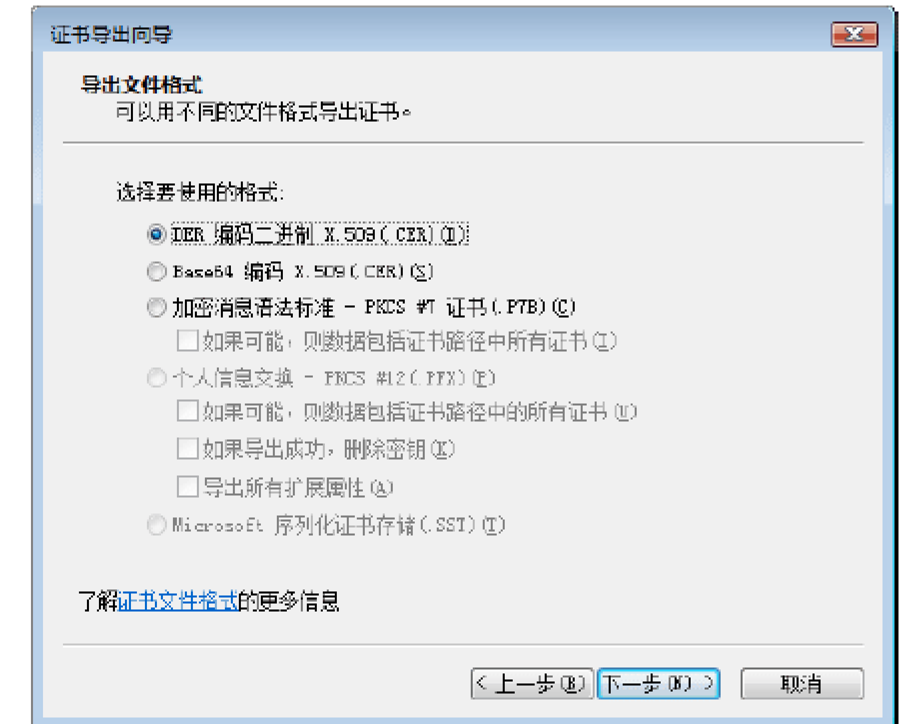


图 10-66 “导出文件格式”界面

⑤ 单击“下一步”按钮，显示如图 10-67 所示的“要导出的文件”界面，在“文件名”文本框中，输入证书的保存路径及文件名。

⑥ 单击“下一步”按钮，显示如图 10-68 所示的“正在完成证书导出向导”界面。

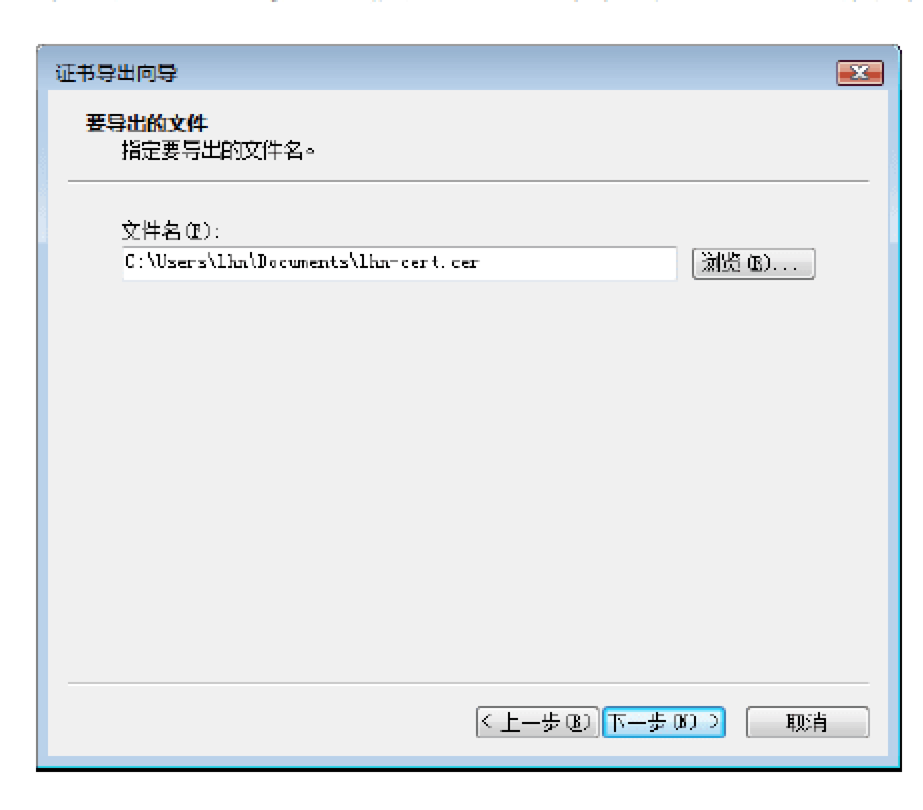


图 10-67 “要导出的文件”界面

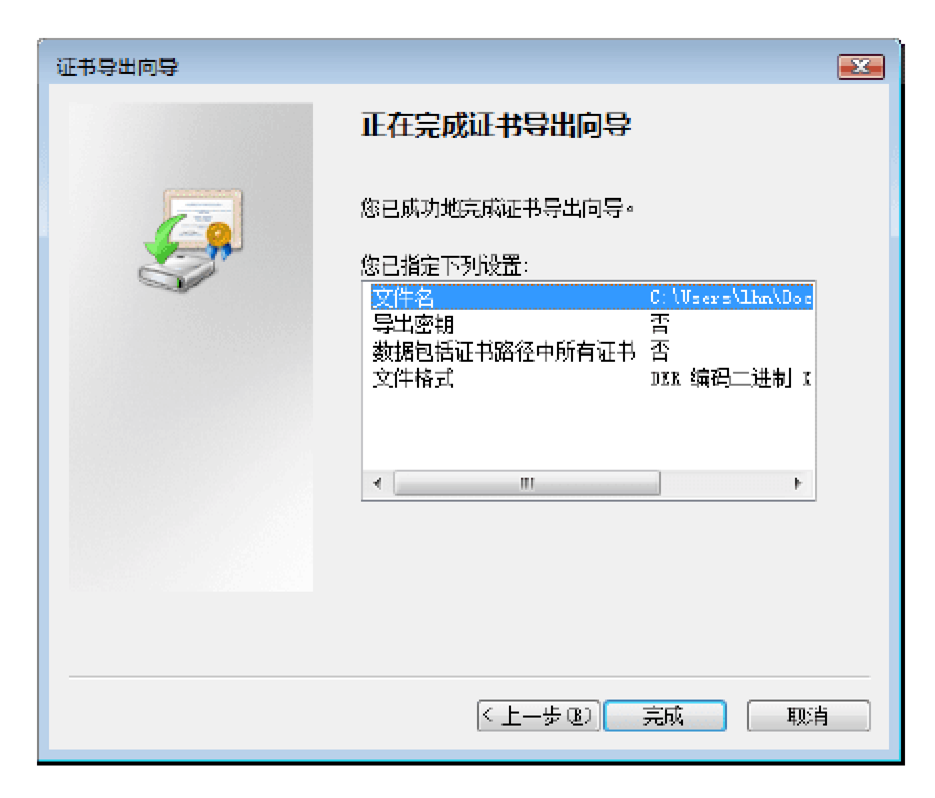


图 10-68 “正在完成证书导出向导”界面

⑦ 单击“完成”按钮，显示如图 10-69 所示的对话框，提示证书导出完成。

⑧ 单击“确定”按钮，完成并关闭向导。

2. 导入证书

① 打开“控制台”窗口，添加“证书”管理单元，展开“个人”，右击“证书”并依次选择快捷菜单中的“所有任务”→“导入”命令，运行“证书导入向导”，如图 10-70 所示。

② 单击“下一步”按钮，显示如图 10-71 所示的“要导入的文件”界面，单击“浏览”按钮，选择以前导出的证书文件。

③ 单击“下一步”按钮，显示如图 10-72 所示的“证书存储”界面，选择证书的存储位置。

④ 单击“下一步”按钮，显示如图 10-73 所示的“正在完成证书导入向导”界面，显示前面所做的配置。

⑤ 单击“完成”按钮，证书导入成功，显示如图 10-74 所示的提示框。

⑥ 单击“确定”按钮，关闭并完成证书导入。

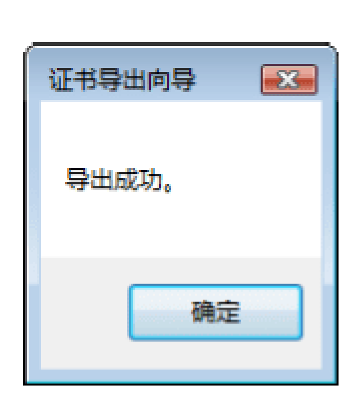


图 10-69 证书导出成功

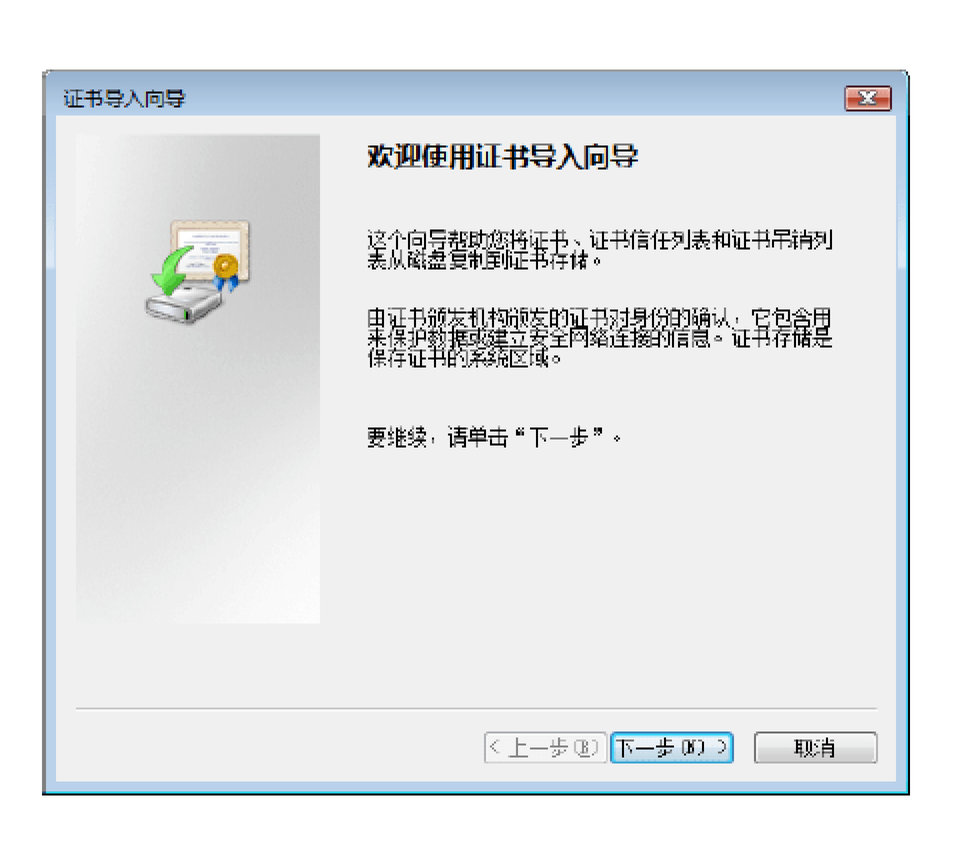


图 10-70 证书导入向导



图 10-71 “要导入的文件”界面

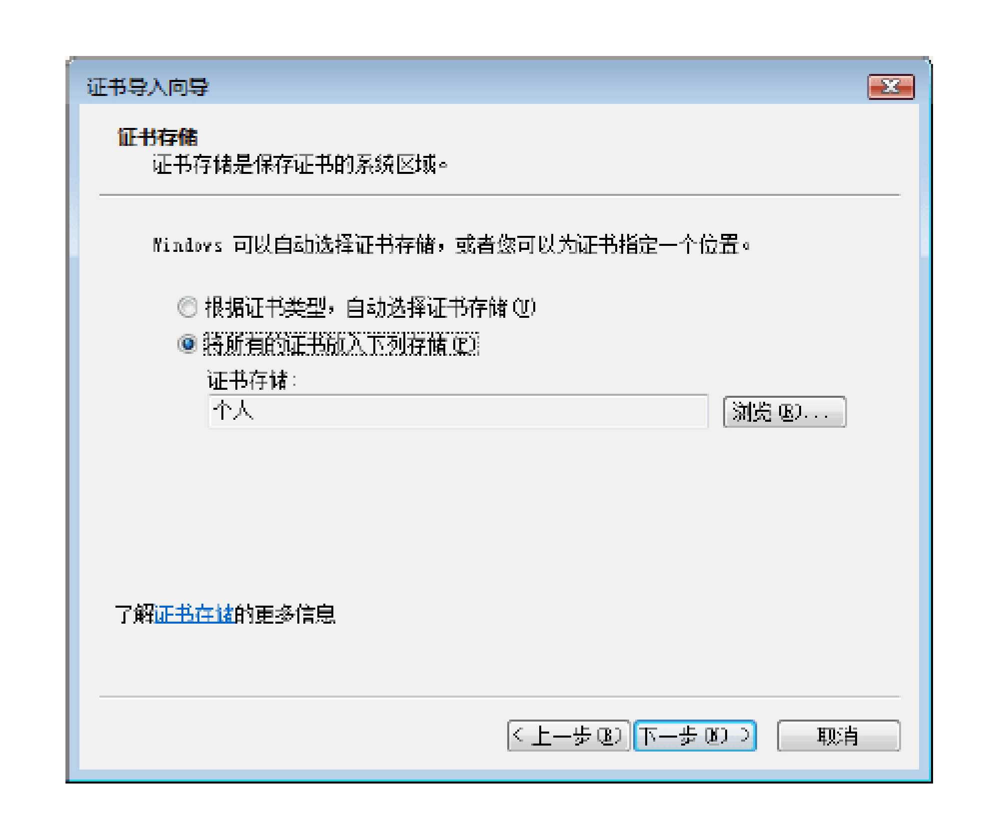


图 10-72 “证书存储”界面

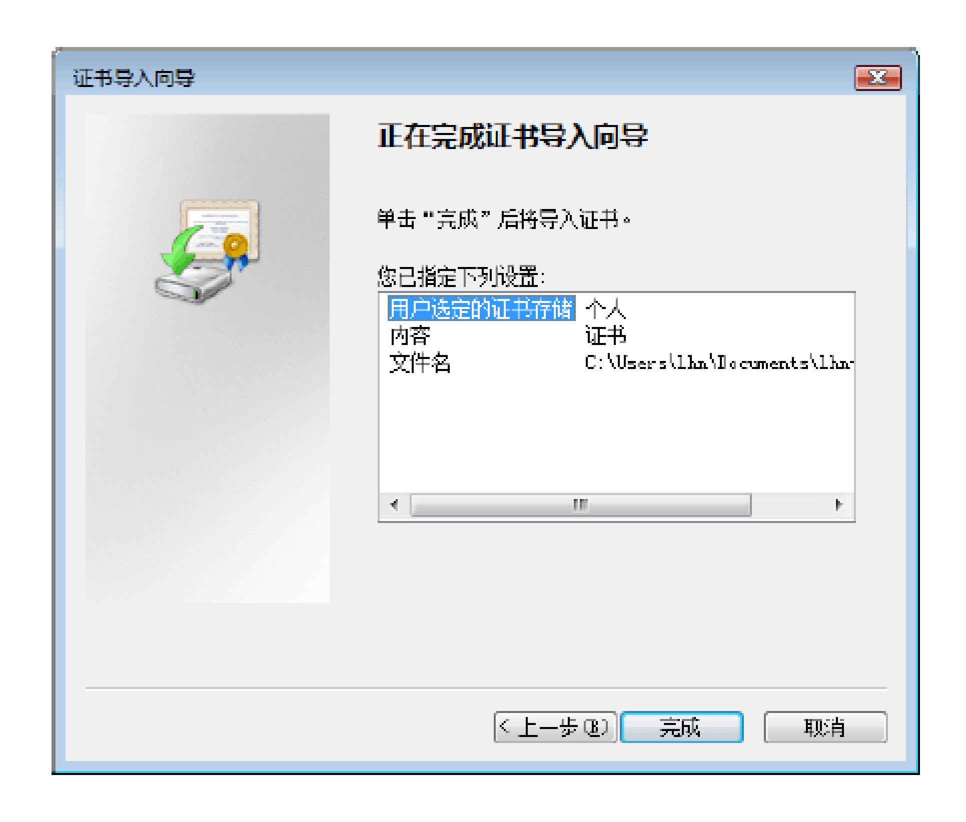


图 10-73 “正在完成证书导入向导”界面



图 10-74 证书导入成功

10.3.5 配置安全 Web 服务器

为了保证数据传输过程中的安全，很多 Web 网站都配置 SSL 安全设置，也就是 HTTPS 网站。不过，

SSL 网站必须使用证书，如果企业中部署了证书服务器，就可以为 Web 服务器申请证书并进行配置。

1. 为 Web 服务器申请证书

为 Web 服务器申请证书有两种方式，一是利用 IE 浏览器申请，二是在 IIS 管理器中利用“创建域证书”来申请。另外，如果是在其他计算机上申请的证书，也可以复制到 Web 服务器上，然后在 IIS 管理器中导入。

(1) 利用 IE 浏览器申请

① 登录到 Web 服务器，在 IE 浏览器中打开证书服务器的证书服务主页，如图 10-75 所示。

② 单击“申请证书”链接，显示如图 10-76 所示的“申请一个证书”界面。

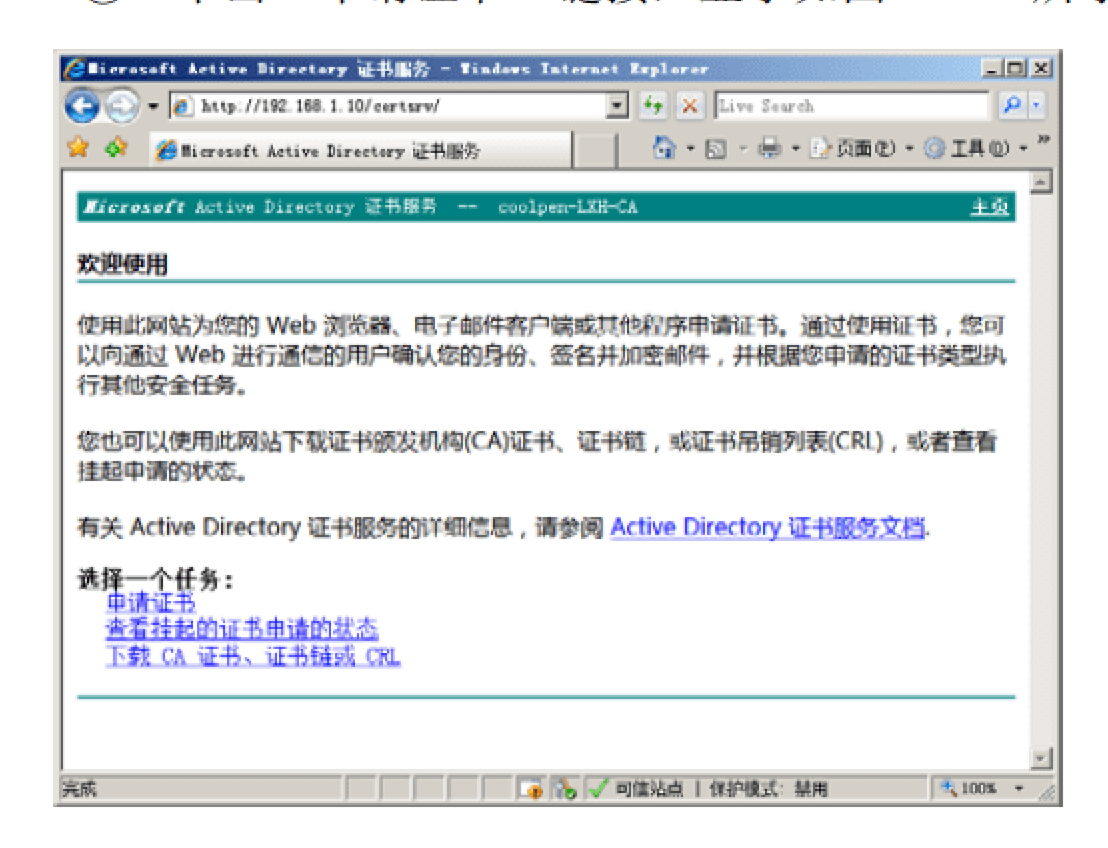


图 10-75 证书服务主页

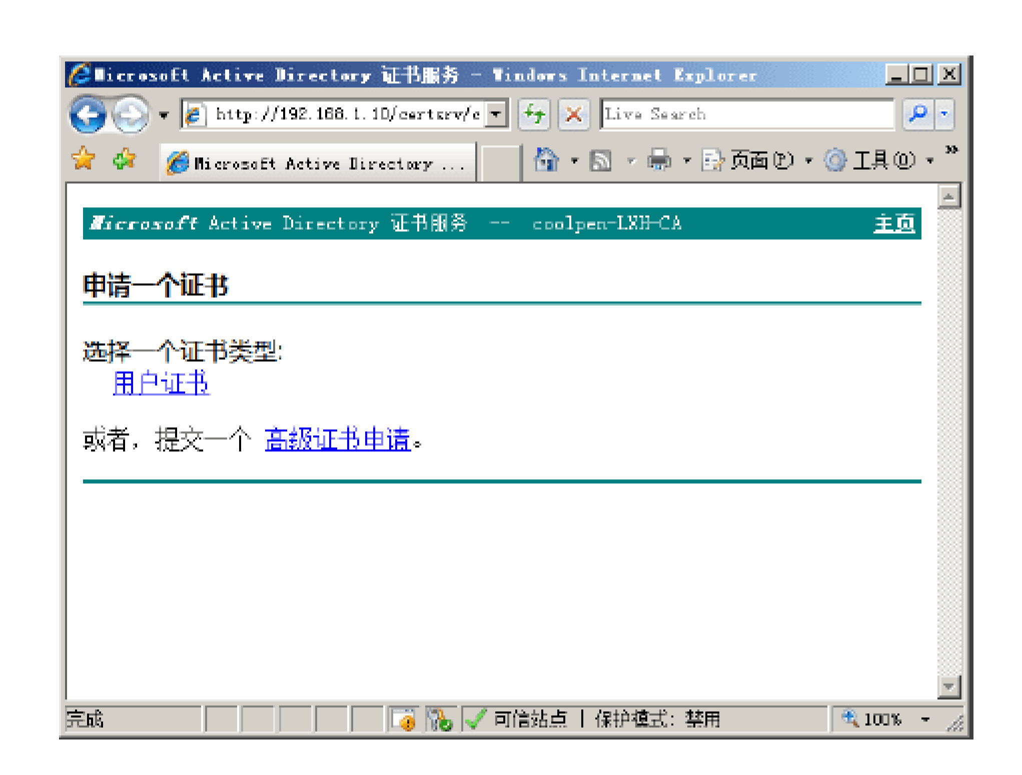


图 10-76 “申请一个证书”界面

③ 单击“高级证书申请”链接，显示如图 10-77 所示的“高级证书申请”界面。

④ 单击“创建并向此 CA 提交一个申请”链接，显示如图 10-78 所示的窗口。在“证书模板”下拉列表框中选择“Web 服务器”选项，并输入识别信息、设置密钥等相关信息。

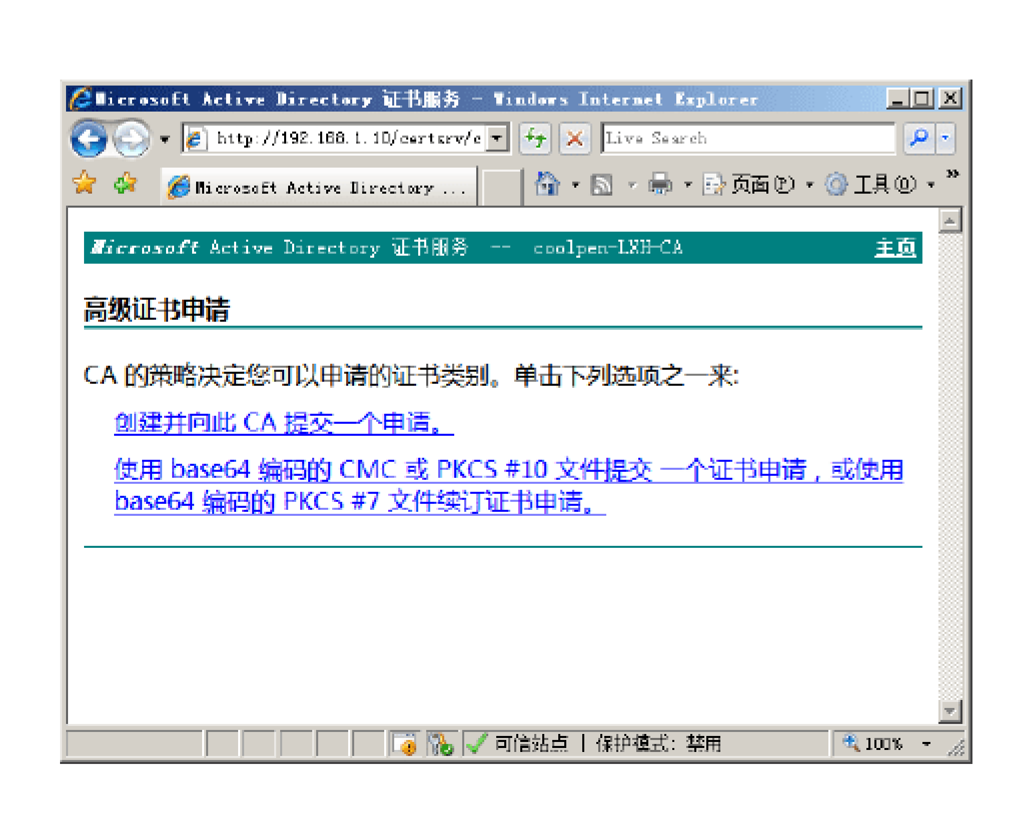


图 10-77 “高级证书申请”界面

图 10-78 申请 Web 证书

⑤ 在窗口底部单击“提交”按钮，开始向证书服务器提交申请。完成后显示如图 10-79 所示的“证书已颁发”界面，提示所申请的证书已颁发。

⑥　单击“安装此证书”链接，即可成功安装此证书，显示如图 10-80 所示的“证书已安装”界面。

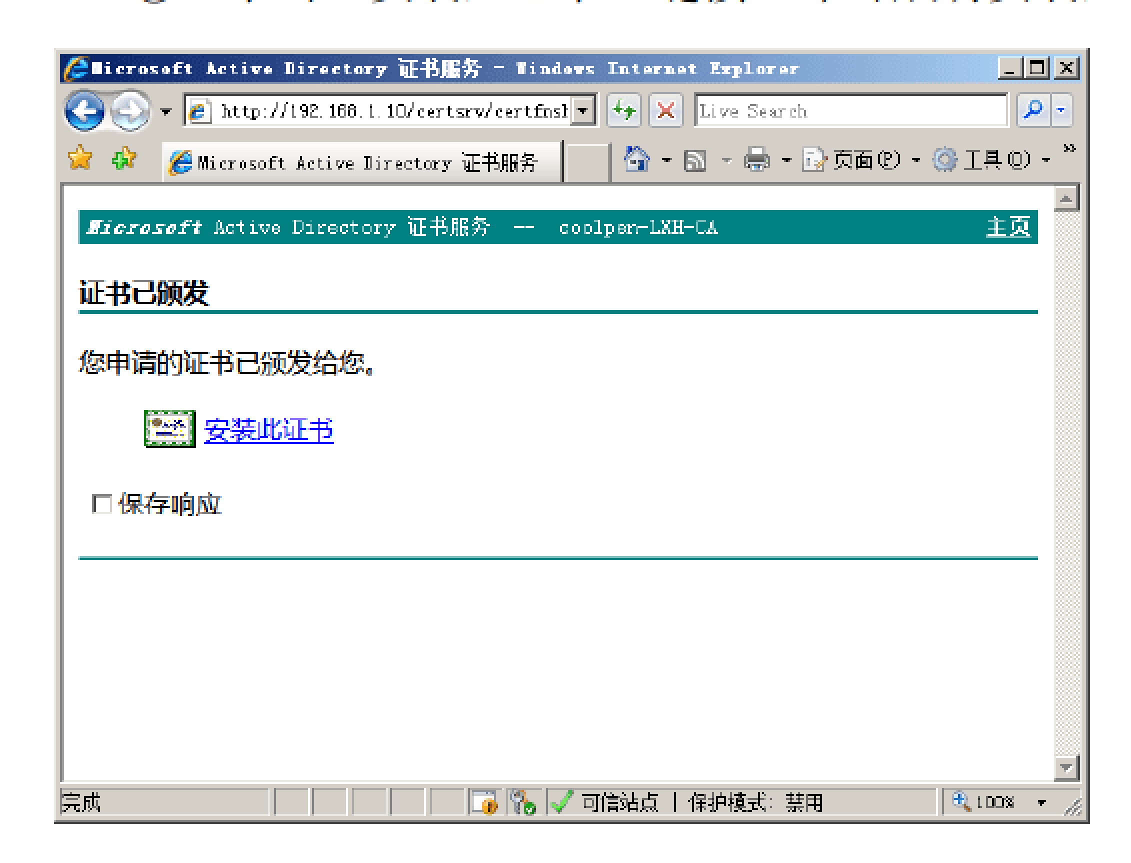


图 10-79　“证书已颁发”界面

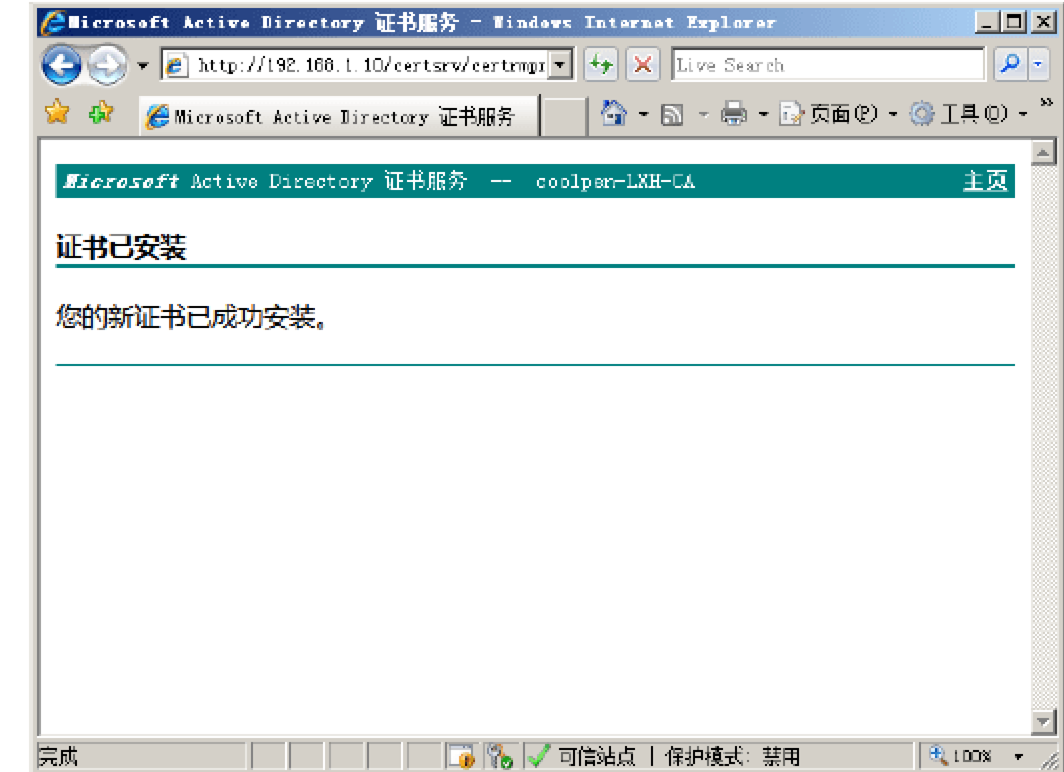


图 10-80　“证书已安装”界面



提示： 如果 Web 服务器没有加入域，则必须先配置信任证书颁发机构。并且，所申请的证书必须由管理员颁发后才能进行安装。

(2)　创建域证书

①　依次选择“开始”→“管理工具”→“Internet 信息服务(IIS)管理器”命令，选择 Web 服务器名称，在“主页”窗口中双击“服务器证书”图标，显示如图 10-81 所示的“服务器证书”窗格。

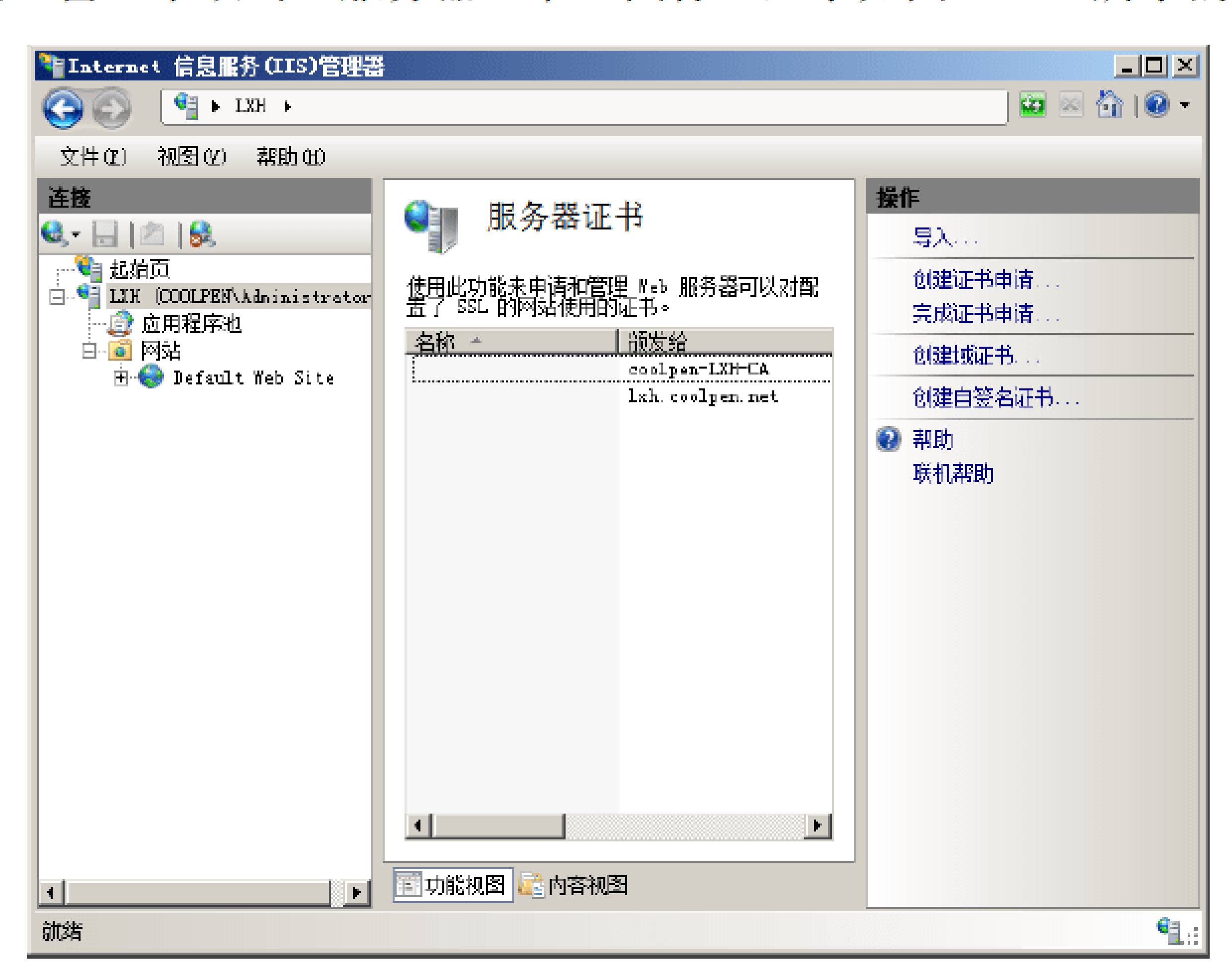


图 10-81　“服务器证书”窗格

②　单击“操作”列表中的“创建域证书”链接，显示如图 10-82 所示的“可分辨名称属性”界面，输入名称、组织、省/市等信息。

③　单击“下一步”按钮，显示如图 10-83 所示的“联机证书颁发机构”界面。

④　单击“浏览”按钮，显示如图 10-84 所示的“选择证书颁发机构”对话框，在列表框中选择证书颁发机构。

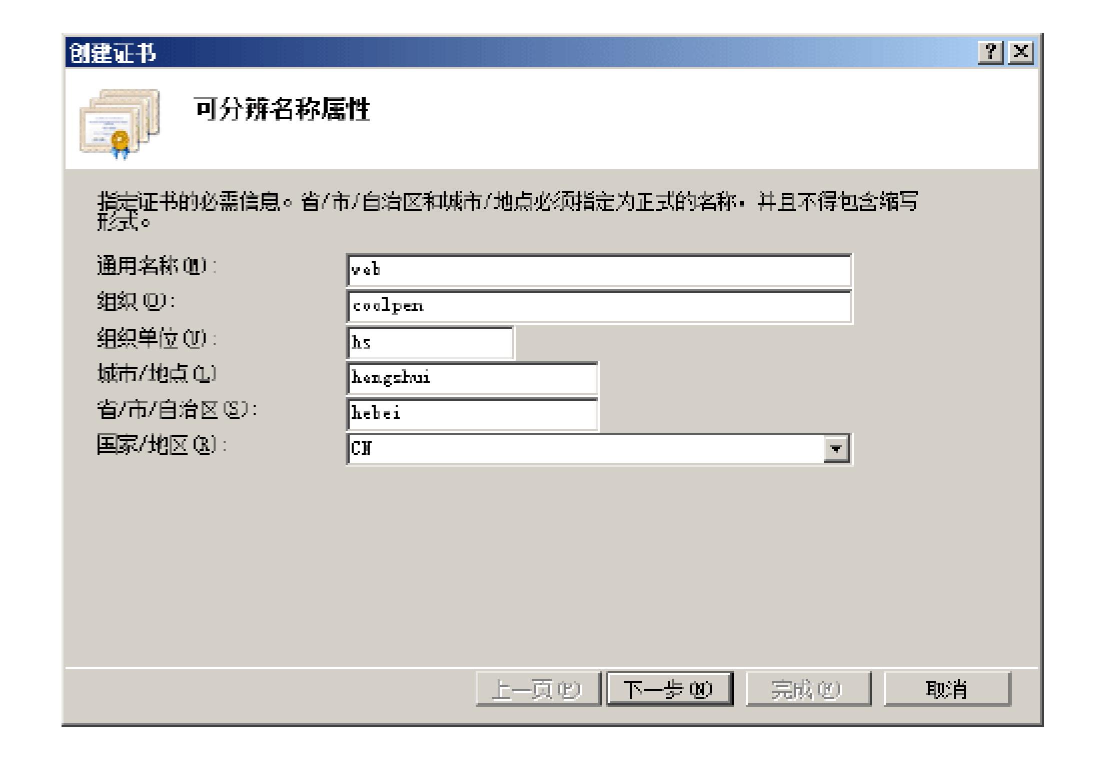


图 10-82 “可分辨名称属性”界面

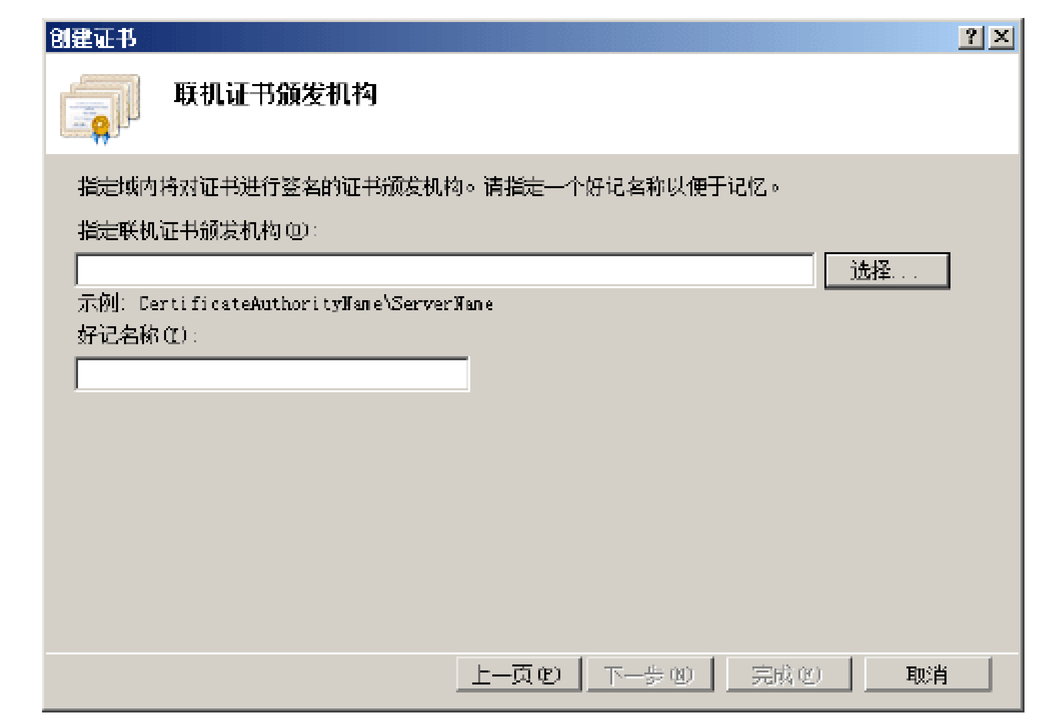


图 10-83 “联机证书颁发机构”界面

⑤ 单击“确定”按钮，返回“联机证书颁发机构”对话框，并在“好记名称”文本框中输入一个名称，如图 10-85 所示。

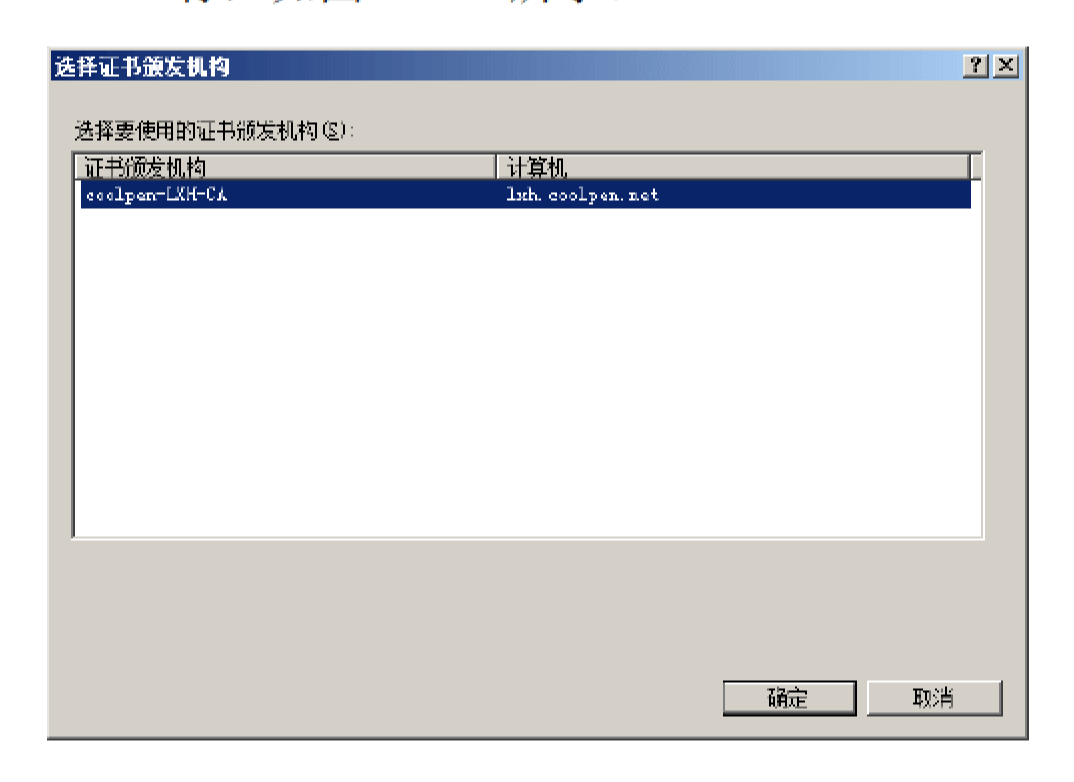


图 10-84 “选择证书颁发机构”对话框



图 10-85 “联机证书颁发机构”界面

⑥ 单击“完成”按钮，证书申请完成，返回到 IIS 管理器窗口。在“服务器证书”窗格中显示了新创建的证书，如图 10-86 所示。

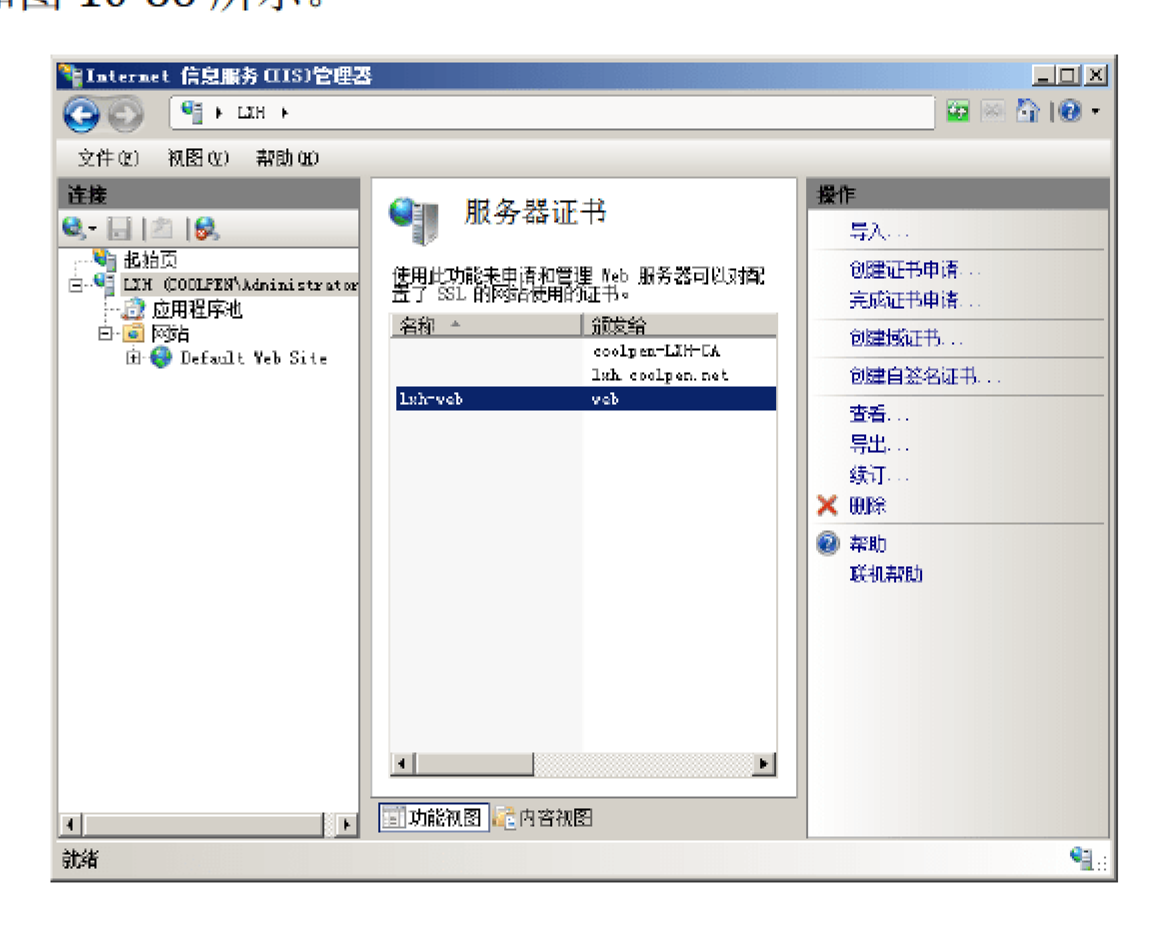


图 10-86 证书创建成功

2. 将证书应用于 Web 服务器

① 在 IIS 管理器窗口中，右击“网站”，选择快捷菜单中的“添加网站”命令，显示如图 10-87 所示的“添加网站”对话框，设置如下选项。

- 网站名称：输入 Web 网站名称。
- 物理路径：指定 Web 网站的主目录。
- 类型：选择 https 选项，创建一个 https 网站。
- IP 地址和端口：指定 IP 地址和端口，默认端口使用 443。
- SSL 证书：在下拉列表中选择为该 Web 网站创建的证书。

② 单击“确定”按钮，完成新网站的创建，如图 10-88 所示。至此，SSL 网站创建完成。

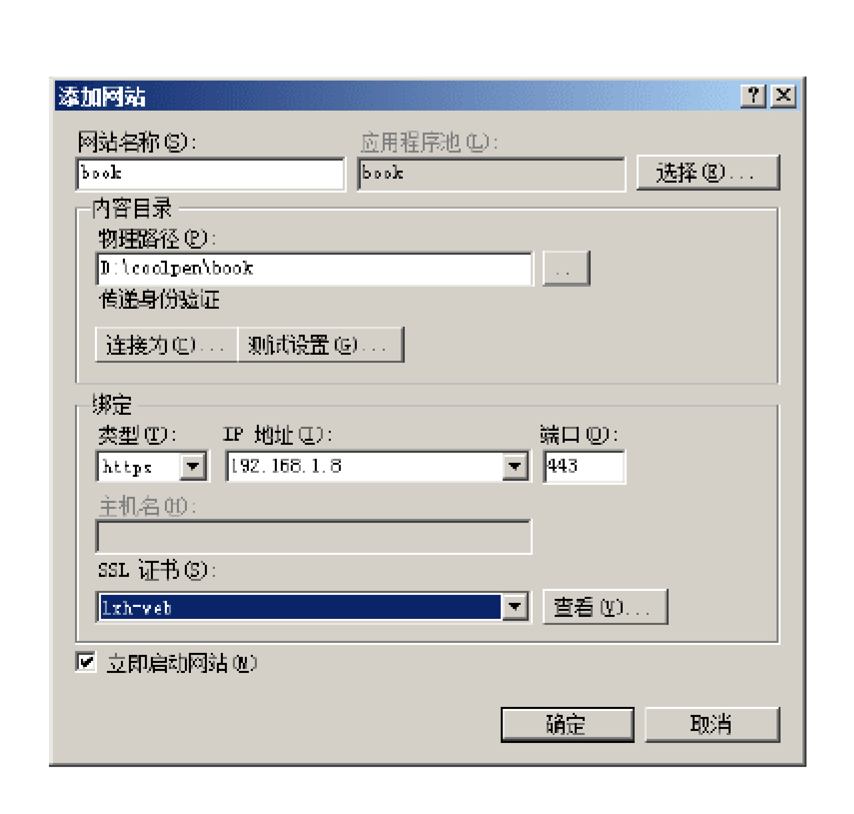


图 10-87　“添加网站”对话框

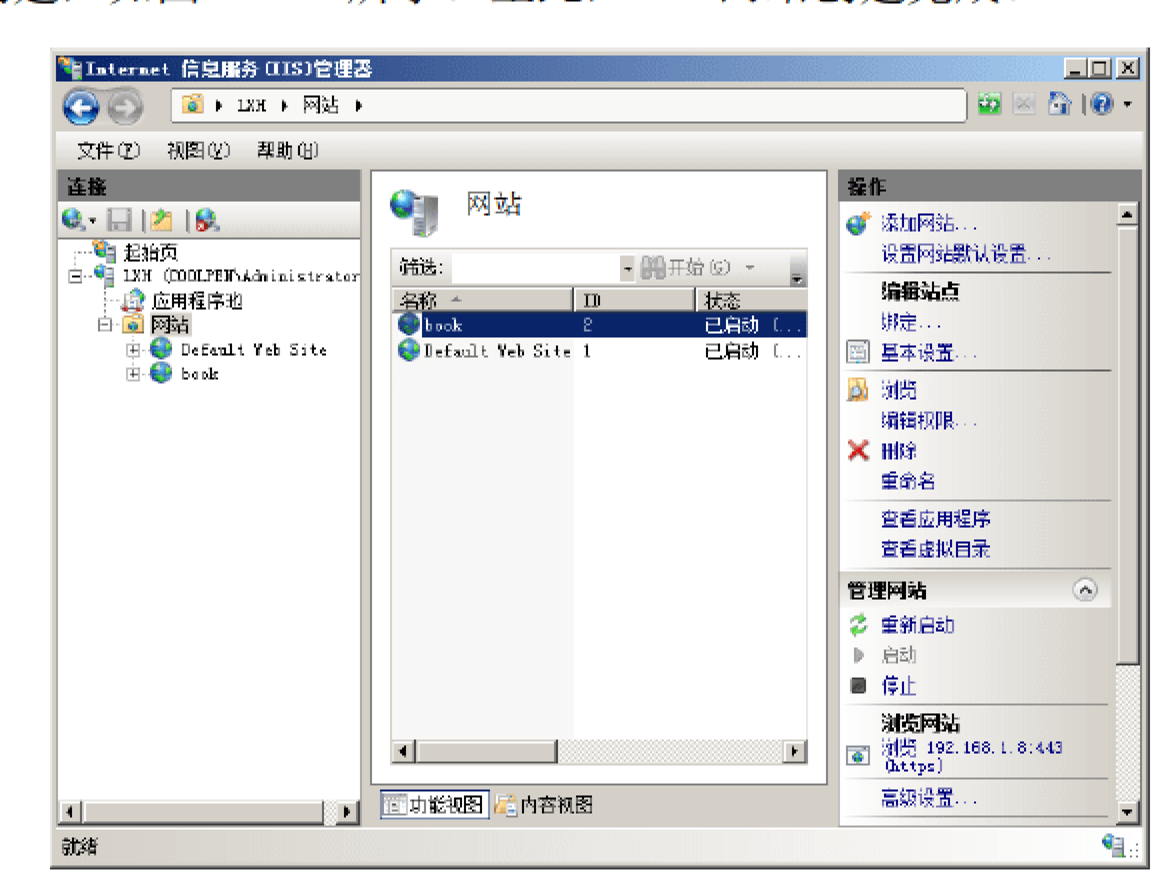


图 10-88　SSL 网站创建完成

3. 在工作站上验证 Web 服务器

如果客户端计算机没有安装证书，那么，当访问 Web 服务器时就会提示证书有问题。只有安装证书后，才能以加密方式浏览 Web 网站。

① 在客户端计算机上打开 IE 浏览器，在地址栏中输入 Web 网站的网站，格式为 https://Web 网站地址，如图 10-89 所示，系统提示“此网站的安全证书有问题”。



图 10-89　提示证书有问题

② 如果要继续浏览此网站，单击“继续浏览此网站(不推荐)”超级链接，显示如图 10-90 所示的窗口。同时，在地址栏中将显示“证书错误”。

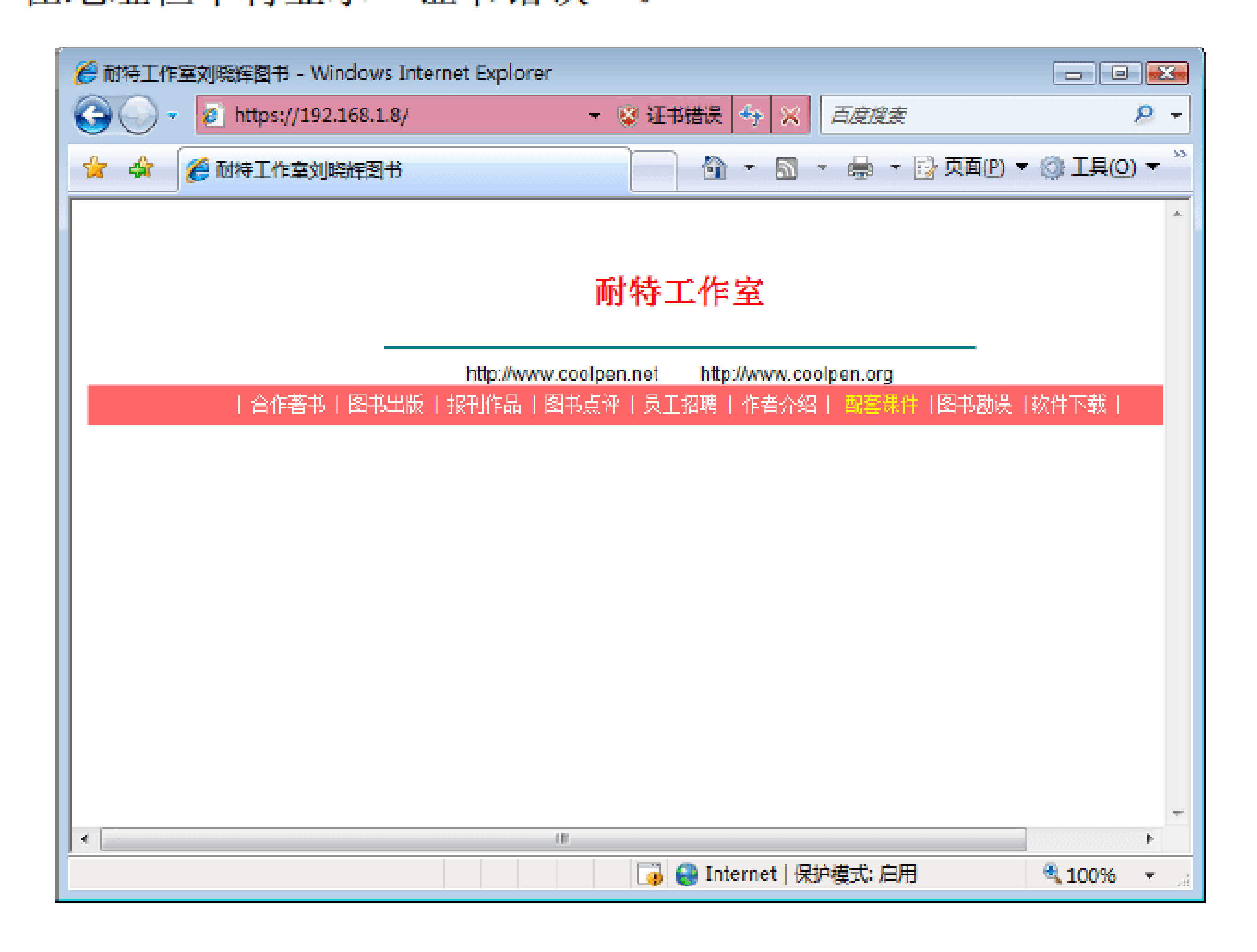


图 10-90　浏览 Web 网站

此时，向证书服务器申请一个证书，或者将证书服务器的证书复制到本地计算机并导入，即可使用安全 Web 方式连接到相应的站点。

第 11 章　远程访问 VPN 连接

远程访问是大多数企业网络中的必备功能，使用户无论出差在外，还是在家办公，都可以通过 Internet 连接公司的内部网络，及时处理各种业务。不过，Internet 传输的开放性很高，安全性也无法保证。VPN(Virtual Private Network，虚拟专用网)是目前常用的远程访问技术之一，其主要特点是安全可靠、机制灵活、费用低廉，易于实现和操作。对于服务器端而言，大多数网络交换机、路由器以及网络管理软件都已经集成 VPN 功能，用户无需增加额外的投资即可享受安全可靠的远程连接。

关键词

- Windows 远程访问 VPN 的组件
- 远程访问 VPN 连接规划和设计
- 配置基于 VPN 的远程访问

11.1 Windows 远程访问 VPN 的组件

VPN 的安全性主要是通过加密实现的。Windows Server 2008 和 Windows Vista 系统支持如下 3 种远程访问 VPN 技术。

- 点对点隧道协议(PPTP)。PPTP 为用户级身份验证使用点对点协议的身份验证，为数据加密使用 Microsoft 点对点加密(MPPE)。
- 使用 Internet 安全协议的第二层隧道协议(L2TP/IPSec)。L2TP/IPSec 为用户级身份验证使用 PPP 身份验证方法，为计算机级身份验证、数据身份验证、数据完整性和数据加密使用 IPSec。
- 安全套接字隧道协议(SSTP)。SSTP 为用户级身份验证使用 PPP 身份验证方法，为数据身份验证、数据完整性和数据加密使用安全套接字层(SSL)通道(也称 TLS 通道)。

Windows 远程访问网络中通常包括图 11-1 所示的 VPN 组件。

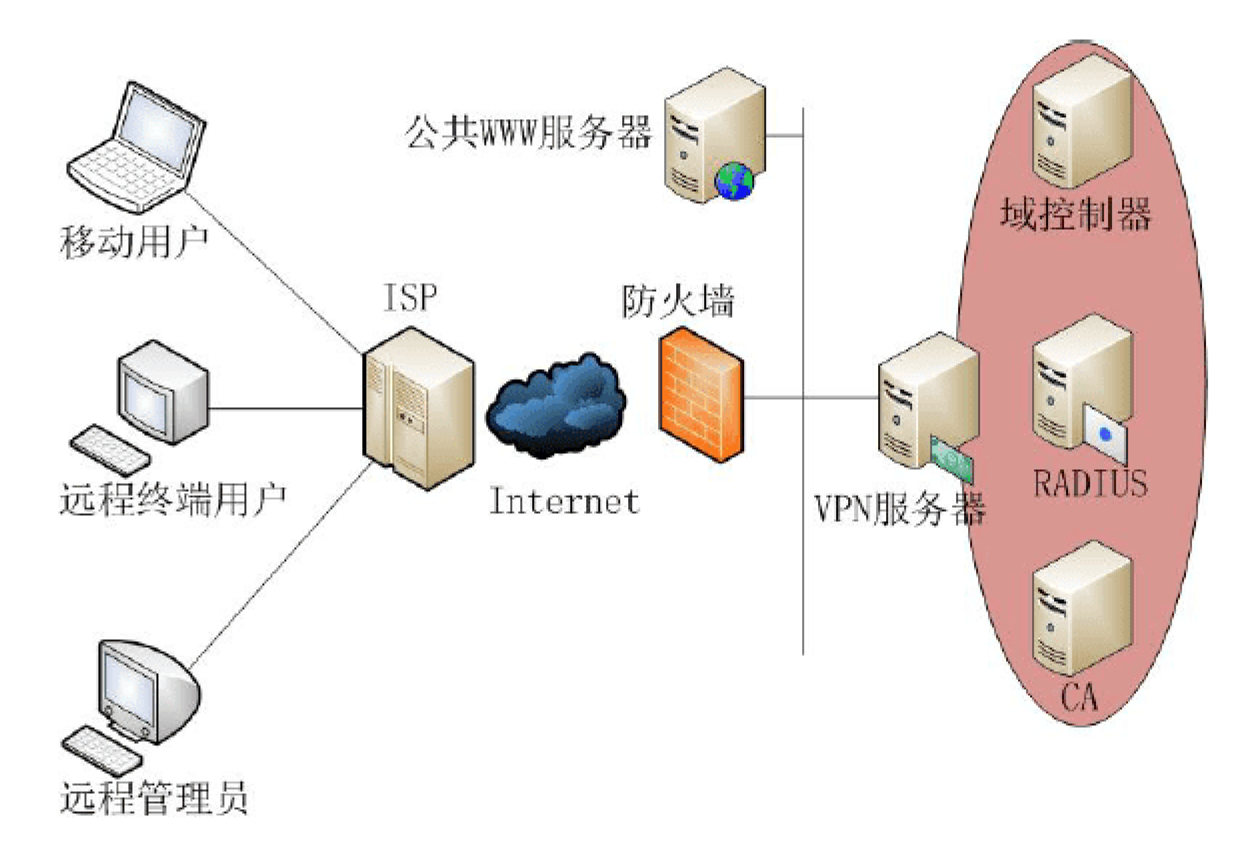


图 11-1　基于 Windows 的远程访问 VPN 的组件

这些组件包括以下内容。

- VPN 客户端。VPN 客户端请求到 VPN 服务器的远程访问 VPN 连接，建立连接后就可以与内网资源进行通信。
- VPN 服务器。VPN 服务器监听远程访问 VPN 连接尝试，强制身份验证和连接请求，并在 VPN 客户端和内网资源间路由数据包。
- RADIUS 服务器。RADIUS 服务器为来自多个 VPN 服务器(以及其他类型的访问服务器)的网络访问尝试提供集中身份验证和授权处理，以及记账功能。
- 活动目录域控制器。活动目录域控制器为身份验证检验用户资格，并提供用户账户信息来评价授权。
- 证书颁发机构(CA)。CA 是 PKI 的一部分，用来为 VPN 客户端发布计算机或用户证书，为 VPN 服务器和 RADIUS 服务器发布计算机证书，以便其进行 VPN 连接的计算机级身份验证和用户级身份验证。

远程访问 VPN 连接的典型用户如下。

- 移动用户：使用笔记本计算机或其他移动终端设备，连接内网访问 E-mail 和其他网络资源。
- 远程终端用户：在家中使用 Internet 访问内网资源。

- 远程管理员：使用 Internet 连接专有网络，并配置网络或应用程序服务。

11.2 远程访问 VPN 连接规划和设计

VPN 的实现方式和应用技术有多种，分别适用于不同的应用环境，并且安全级别和易用程度也略有不同，没有一种 VPN 方案是放之四海而皆准的。因此，部署远程访问 VPN 连接之前，必须进行周密规划，寻求一种最佳解决方案；需要考虑的因素通常包括加密协议、身份验证方式、服务器类型等。

11.2.1 VPN 协议

Windows Server 2008 支持如下远程访问 VPN 协议。

- PPTP：PPTP 使用 PPP 用户身份验证和 MPPE 加密。当使用具有强壮密码的 MS-CHAP v2 或 PEAP-MS-CHAP v2 时，PPTP 是一种安全的 VPN 技术。对于基于证书的身份验证，EAP-TLS 可与基于注册的证书或智能卡一同使用。PPTP 被广泛支持，易于配置，可用于大部分网络地址转换(NAT)。Windows Server 2008、Windows Vista、Windows Server 2003 和 Windows XP 均支持 PPTP。
- L2TP/IPSec：L2TP 利用 PPP 用户身份验证和 IPSec 数据包保护。L2TP/IPSec 使用证书(默认)和 IPSec 计算机级的身份验证过程来协商受保护的 IPSec 会话，然后基于 PPP 的用户身份验证来认证 VPN 客户端计算机的用户。通过使用 IPSec，L2TP/IPSec 为每个数据包提供了数据机密性(加密)、数据完整性(证明数据没有在传输过程中被修改)和数据的原始认证(证明数据由授权用户发出)。但是 L2TP/IPSec 需要 PKI 为每个基于 L2TP/IPSec 的 VPN 客户端分配计算机证书。Windows Server 2008、Windows Vista、Windows Server 2003 和 Windows XP 均支持 L2TP/IPSec。
- SSTP：SSTP 利用 PPP 用户身份验证，为封装和加密使用 SSL 上的 HTTP 通道。因为 SSTP 使用 SSL 通信(使用 TCP 端口 443)，所以 SSTP 可用于多种不同的网络配置，如位于 NAT、防火墙或不支持 PPP 或 L2TP/IPSec 通信的代理服务器之后的 VPN 客户端或服务器。只有 Windows Server 2008 和 Windows Vista SP1 支持 SSTP。

1. VPN 协议的设计

为远程 VPN 连接选择加密协议时，应遵循如下原则。

- 当使用 PEAP-MS-CHAP v2、EAP-MS-CHAP v2 或 MS-CHAP v2 身份验证时，PPTP 不需要证书基础结构来为每个 VPN 客户端发布证书。
- 基于 PPTP 的 VPN 连接为数据包提供数据机密性(加密)。基于 PPTP 的 VPN 连接不提供数据完整性或数据原始认证。
- 通过使用 IPSec，基于 L2TP/IPSec 的 VPN 连接提供数据机密性、数据完整性和数据原始认证。
- 基于 SSTP 的 VPN 连接客户端和服务器可置于 NAT、防火墙或 Web 代理之后。但是，SSTP 不支持位于身份验证 Web 代理之后的 VPN 客户端和服务器。
- 默认情况下，运行 Windows Server 2008 的 VPN 服务器同时支持这 3 种 VPN 连接类型。对于没有安装计算机证书的 VPN 客户端，用户可以使用 PPTP；对于安装了计算机证书的 VPN 客户端，用户可以使用 L2TP/IPSec；对于运行 Windows Vista SP1 的 VPN 客户端使用 SSTP。
- 如果用户正在联合使用 VPN 协议，用户可以为 PPTP、L2TP/IPSec 或 SSTP 连接创建单独的网络

策略，定义不同的连接设置。

- 在 Windows Server 2008 和 Windows Vista 中，IPv6 通信可通过基于 PPTP 的 VPN 连接作为 IPv4 隧道通信进行发送，或者在 VPN 隧道中进行本地 IPv6 通信。
- 在 Windows Server 2008 和 Windows Vista 中，L2TP/IPSec 或 SSTP 的 VPN 连接支持作为 IPv4 隧道通信的 IPv6 通信、VPN 隧道内的 IPv6 通信，以及 IPv6 之上的 VPN 连接。

2. VPN 协议的需求

如果在 NAT 网络中使用一个 NAT 编辑器来传输 PPTP 通道数据，则基于 PPTP 的 VPN 客户端可以位于 NAT 之后。大部分 NAT 网络使用单一公有 IPv4 地址，包括 ICS 和 NAT 路由协议组件，可以被配置为允许基于 IPv4 地址和 TCP、UDP 端口的入站通信。但是，PPTP 通道数据不能使用 TCP 或 UDP 的头。所以，当使用单一公有 IPv4 地址时，VPN 服务器不能位于使用 ICS 或 NAT 路由协议组件的计算机之后。

如果基于 L2TP/IPSec 的 VPN 客户端或服务器都支持 IPSec NAT 穿越(NAT-T)，则服务器或客户端不能位于 NAT 之后。Windows Server 2008、Windows Vista、Windows Server 2003 和 Windows XP SP2 都支持 IPSec NAT-T。

L2TP/IPSec 默认情况下支持计算机证书，并推荐使用 IPSec 身份验证方式。尽管用户可以配置为认证的 L2TP/IPSec 连接配置一个预共享密钥，但是这并不推荐，除非作为在配置 PKI 时的过渡身份验证方式。计算机证书身份验证需要 PKI 来发行计算机证书给 VPN 服务器计算机和所有 VPN 客户端计算机。

Windows Server 2008 和 Windows Vista SP1 支持 SSTP。SSTP 使用加密的 SSL 通道来保护所有通过 VPN 连接的数据。为了创建该加密通道，VPN 服务器必须拥有计算机证书，并且 VPN 客户端计算机必须能够验证 VPN 服务器的计算机证书。这就意味着 VPN 客户端必须拥有发布 VPN 服务器计算机证书的 CA 的根 CA 证书。

如果用户想要在 VPN 通道中发送原始 IPv6 通信，或者使用 IPv6 Internet 中要求拨号的 VPN 连接，则必须使用 L2TP/IPSec。



注意： 如果用户已经拥有一个 PKI，则可以使用 L2TP/IPSec 代替 PPTP。如果用户没有使用所有的 VPN 协议，则在“路由和远程访问”管理单元中的“端口”节点中配置不使用的 VPN 协议的端口值为 0。

11.2.2 身份验证方式

VPN 连接中可以通过多种方式实现对客户端的身份验证。Windows Server 2008 支持的身份验证协议如下。

- MS-CHAP v2
- EAP-MS-CHAP v2
- EAP-TLS
- PEAP-MS-CHAP v2
- PEAP-TLS

1. 身份验证协议的设计选择

选择身份验证协议时，应遵循如下设计原则。

- EAP-TLS 和 PEAP-TLS 必须与 PKI 联合使用。对于 EAP-TLS，VPN 客户端发送自己的用户证书进

行身份验证，并且身份验证服务器发送计算机证书进行身份验证。默认情况下，VPN 客户端认证 VPN 服务器的证书。对于 PEAP-TLS，VPN 客户端和认证服务器创建一个加密的 TLS 通道，然后 VPN 客户端和认证服务器交换证书。EAP-TLS 和 PEAP-TLS 都比 PEAP-MS-CHAP v2 或 MS-CHAP v2 安全。

- 如果没有用户证书或智能卡，则可以使用 PEAP-MS-CHAP v2、MS-CHAP v2 或 EAP-MS-CHAP v2。推荐使用 PEAP-MS-CHAP v2，因为 PEAP-MS-CHAP v2 消息交换是受 TLS 通道保护的，使恶意攻击者很难截获交换消息，确定用户密码。
- MS-CHAP v2、EAP-MS-CHAP v2 和 PEAP-MS-CHAP v2 都是基于密码的身份验证协议。
- EAP-TLS 和 PEAP-TLS 都是基于证书的身份验证协议。
- 对于基于 L2TP/IPSec 的连接，任一用户级别的身份验证协议都可以使用，因为在 VPN 客户端和 VPN 服务器确定 IPSec 保护通道之后才进行身份验证。但是，推荐 PEAP-MS-CHAP v2、MS-CHAP v2、EAP-MS-CHAP v2、EAP-TLS 或 PEAP-TLS 为强壮用户提供身份验证。

2. 身份验证协议的要求

如果已经选择了不同的 VPN 连接加密协议，则选择身份验证协议时，应考虑如下问题。

- 如果是基于 PPTP 协议加密的 VPN 连接，则用户必须使用 MS-CHAP v2、EAP-MS-CHAP v2、PEAP-MS-CHAP v2、EAP-TLS 或 PEAP-TLS。只有这些身份验证协议提供产生会话初始化加密密钥的机制，才能用于 VPN 客户端和 VPN 服务器加密 PPTP 数据。
- 运行 Windows Server 2008 和 Windows Vista 的 VPN 客户端都支持 PEAP-MS-CHAP v2 和 EAP-MS-CHAP v2。运行 Windows Server 2008、Windows Vista、Windows Server 2003 或 Windows XP 的 VPN 客户端都支持 MS-CHAP v2。
- PEAP-MS-CHAP v2 要求在身份验证服务器上安装计算机证书和 VPN 客户端计算机所使用的计算机证书的根 CA 证书。只有运行 Windows Server 2008 或 Windows Vista 的 VPN 客户端支持 PEAP-MS-CHAP v2。
- 对于基于 SSTP 的连接，用户必须使用 MS-CHAP v2、EAP-MS-CHAP v2、PEAP-MSCHAP v2、EAP-TLS 或 PEAP-TLS。只有这些身份验证协议提供产生会话初始化加密密钥的机制，才能避免恶意攻击者对基于 SSTP 的 VPN 连接的攻击。
- 为了配置 NAP 的 VPN 强制，用户必须使用基于 PEAP 的身份验证方式。



注意：如果使用基于密码的身份验证协议，则需要在网络中使用强密码，即长度至少为 8 个字符，且包含大小写字母、数字和标点符号。

11.2.3　VPN 服务器

VPN 服务器端有多种实现方式，例如路由器或防火墙上的 VPN 模块、Windows 服务器操作系统的服务器等。从易用性和实现成本来考虑，建议选择基于 Windows Server 2008 或 Windows Server 2003 系统组件的 VPN 服务器。

1. VPN 服务器的设计选择

在 Windows Server 2008 或 Windows Server 2003 系统中，安装 VPN 服务器组件时，应遵循如下设计原则。

- VPN 客户端既可以从 DHCP 获取 IP 地址，也可以从手动配置的地址范围中获取 IP 地址。使用 DHCP 获取 IP 地址简化了配置，但是，用户必须确保 VPN 服务器所在子网的 DHCP 范围为所有连接子网的计算机拥有足够的地址和远程访问客户端的最大数量。如果用户配置了静态地址池，可能需要其他路由配置。
- VPN 服务器可以评估身份验证和 VPN 连接的授权，或者依赖 RADIUS 服务器。当配置 VPN 服务器时，用户可以为身份验证或记账选择使用 Windows 或 RADIUS。
- 当配置使用 Windows 来进行身份验证和记账时，VPN 服务器是活动目录域的成员，并且通过与域控制器通信来验证 VPN 客户端的证书，获取 VPN 客户端拨号属性。默认情况下，VPN 服务器记录 VPN 连接记账信息在本地记账日志文件中。当配置为使用 RADIUS 进行身份验证和记账时，VPN 服务器使用 RADIUS 服务器来验证 VPN 客户端的证书，授权连接尝试，并且记录 VPN 连接记账信息。
- “路由和远程访问服务器安装向导”不能为远程访问 VPN 客户端自动启用 IPv6 支持。

2. VPN 服务器的要求

基于 Windows Server 2008 系统远程访问功能的 VPN 连接，有如下配置要求。

- VPN 服务器的 Internet 接口和内网接口必须拥有静态 IP 地址。由于存在默认路由冲突的可能性，用户应该使用 IPv4 地址手动配置内网接口、子网掩码、DNS 服务器和 WINS 服务器。但是，不要配置 VPN 服务器内网接口的默认网关。这样才可能使 VPN 服务器拥有手动 TCP/IP(IPv4)配置，并且使用 DHCP 获取 IPv4 地址。
- 对于使用 PEAP-MS-CHAP v2、EAP-TLS 或 PEAP-TLS 身份验证协议的 VPN 连接，用户必须在身份验证服务器上安装 VPN 客户端可以验证的计算机证书。也可能需要用户在 VPN 客户端上安装身份验证服务器的计算机证书的发行 CA 的根 CA 证书。
- 对基于 SSTP 的 VPN 连接，用户必须在 VPN 服务器上安装 VPN 客户端可以验证的计算机证书。用户也可能需要在 VPN 客户端上安装 VPN 服务器的计算机证书的发行 CA 的根 CA 证书。
- 对基于 L2TP/IPSec 的 VPN 连接，用户必须在 VPN 服务器上安装 VPN 客户端可以验证的计算机证书。
- 如果用户为本地身份验证或为 RADIUS 身份验证配置 VPN 服务器，并且 RADIUS 服务器是运行 NPS 的计算机，则默认网络策略将会拒绝所有类型的连接尝试，除非远程访问允许的用户账户拨号属性是允许访问的。如果用户想要为 VPN 连接使用该网络策略，则设置策略类型为“允许访问”。如果用户想要通过组或连接类型管理授权和 VPN 连接设置，则必须配置其他 NPS 策略。

11.2.4 Internet 基础结构

VPN 客户端和服务器之间的通信是借助 Internet 实现的，因此部署 VPN 远程访问之前，必须确保 VPN 服务器是公开在 Internet 中的，并且在 Windows 防火墙或网管防火墙上允许所有 VPN 出站连接。

1. VPN 服务器名称的可解析性

在大部分情况下，用户都是通过 FQDN 来涉及 VPN 服务器的，而非 IPv4 或 IPv6 地址。只要 FQDN 名称可以解析为 IPv4 或 IPv6 地址，用户就可以使用 FQDN。所以，必须确保当配置 VPN 连接时，VPN 服务器所使用的名称可以解析为 DNS 服务器所使用的 IPv4 或 IPv6 地址。

当用户使用名称而非地址时，如果多个 VPN 服务器使用相同的 DNS 主机名称，也可以利用 DNS 循环

负载平衡。在 DNS 中，用户可以创建多个记录，解析指定的主机名称为不同的 IPv4 地址。在这种情况下，DNS 服务器返还所有地址回应 DNS 名称查询，并且通常对于连续的查询随机排列地址的顺序。由于大部分的 DNS 客户端使用 DNS 查询回应的第一个地址，这样 VPN 客户端连接就可以平均到所有 VPN 服务器上，只要所有 VPN 服务器都可用。



提示：为了确保 VPN 服务器的可用性，用户可以使用网络负载平衡。

2. VPN 服务器的可到达性

为了可到达性，VPN 服务器必须分配一个公有 IPv4 地址或者全局 IPv6 地址。如果被分配一个静态公有 IPv4 地址或全局 IPv6 地址前缀，通常情况下不会出现问题。在一些 IPv4 配置中，VPN 服务器实际上使用专有 IPv4 地址配置，并且拥有公有的静态 IPv4 地址。在 Internet 和 VPN 服务器之间的设备将 VPN 服务器的公有和有效 IPv4 地址转换为数据包发送到 VPN 服务器。

尽管路由基础结构能提供到达性，但是 VPN 服务器可能由于防火墙、数据包筛选器路由器、NAT、安全网关或其他类型的设备的配置，而无法到达。

3. VPN 服务器和防火墙配置

VPN 服务器支持如下两种防火墙规划方案。

- VPN 服务器可以直接到达 Internet，并且防火墙位于 VPN 服务器和内网之间。这种配置下，VPN 服务器必须使用数据包筛选器配置，只允许 VPN 通信进出 Internet 接口。防火墙可以配置为允许指定类型的远程访问通信。
- VPN 服务器通过防火墙到达 Internet，并且 VPN 服务器位于防火墙和内网之间。这种配置下，防火墙和 VPN 服务器都可以到达名为边界网络的子网。防火墙和 VPN 服务器必须配置为只允许 VPN 进出站连接。

4. 对 Internet 基础结构的要求

VPN 连接对 Internet 基础结构的要求如下。

- 确保 VPN 服务器的 FQDN 的可解析性，放置适当的 DNS 地址(A)或 IPv6 地址(AAAA)记录在 DNS 服务器或 ISP 的 DNS 服务器中。当直接连接到 IPv4 或 IPv6 Internet 时使用 Ping 工具测试解析性。
- 确保 VPN 服务器的 IPv4 或 IPv6 地址从 Internet 可以到达，当直接连接 Internet 时，这个过程可以通过使用 Ping 工具来 Ping VPN 服务器的域名或 IP 地址来完成。如果显示 Destination unreachable 的错误消息，则 VPN 服务器是不可到达的。



注意：需要为 PPTP、L2TP、SSTP 或连接 Internet 和边界网络的适当防火墙，以及 VPN 服务器接口的所有类型的通信，配置数据包筛选器。

11.2.5　内网基础结构

内网基础结构确保 VPN 客户端可以与内网中使用 VPN 服务器作为 IPv4 或 IPv6 路由器的节点交换数据包。如果没有适当的内网基础结构设计，VPN 服务器可能无法完成如下工作。

- 解析网络中的设备或网络名称。
- 获取内网可到达的 IPv4 地址或 IPv6 子网前缀。
- 到达内网中的指定目标。

1. 内网名称解析

确保每台 VPN 服务器已经正确配置内网 DNS 服务器的 IP 地址，如果用户使用 WINS 解析内网 NetBIOS 名称，则 VPN 服务器还需要配置内网 WINS 服务器的 IPv4 地址。VPN 服务器应该手动配置 DNS 服务器和 WINS 服务器。

作为 PPP 连接协商 IPv4 过程的一部分，VPN 客户端接收 DNS 和 WINS 服务器的地址。默认情况下，VPN 客户端继承 VPN 服务器上配置 DNS 和 WINS 服务器地址。在 PPP 连接协商完成后，运行 Windows Server 2008/2003 或 Windows XP/Vista 的 VPN 客户端发送 DHCP 请求到 DHCP 服务器。

如果 VPN 服务器使用 DHCP 配置内网接口(不推荐)，那么当路由和远程访问服务器向导运行时，VPN 服务器中转 DHCP 请求到 DHCP 服务器。如果 VPN 服务器在内网接口中使用静态 TCP/IP 配置(推荐)，那么 DHCP 中转代理路由协议组件必须使用至少一个 DHCP 的 IPv4 地址进行配置。用户可以添加 DHCP 服务器的 IPv4 地址到 DHCP 中转代理路由协议组件中。

为了动态配置 VPN 连接的 DNS 的 IPv6 地址，基于 Windows Vista 或 Windows Server 2008 的 VPN 客户端依赖 VPN 服务器发送的路由广播消息。如果路由广播消息具有其他状态配置信息，则 VPN 客户端发送 DHCPv6 请求到 VPN 服务器。如果 Windows Server 2008 VPN 服务器使用 DHCPv6 中转代理配置，那么 Information-Request 消息将会被转发到 DHCPv6 服务器。DHCPv6 中转消息转发回 VPN 客户端，并且包含 DNS 服务器的地址。

管理员在配置 VPN 服务器时应注意如下问题。

- 预先使用 Ping 和 Net 工具，在 VPN 服务器上测试内网 DNS 和 WINS 名称解析的连接和运行情况。如果名称解析在 VPN 服务器上不能正常工作，则在 VPN 客户端上也无法工作。
- 由于 VPN 服务器的内网接口使用 TCP/IP 手动配置，路由和远程访问服务器安装向导不能自动配置 DHCP 中转代理路由协议组件。用户必须手动添加内网中至少一个 DHCP 服务器的 IP 地址到 DHCP 中转代理组件中；否则，VPN 客户端不会接收到更新的 DNS 和 WINS 服务器的地址。
- 如果用户拥有不具有 DHCP、DNS 或 WINS 服务器的单独子网，则必须配置 DNS 服务器或 WINS 服务器，为局域网中的计算机和 VPN 客户端提供名称解析功能，或者启用 NetBIOS 广播名称解析。为了启用 NetBIOS 广播名称解析，在“路由和远程访问”管理单元中，在 VPN 服务器的属性对话框的“IPv4”选项卡中，选中“启用广播名称解析”复选框。
- 为了在 VPN 客户端和 DHCPv6 内网服务器之间转发 DHCPv6 消息，必须添加和配置 DHCPv6 中转代理路由协议组件。



注意：为了确保 VPN 客户端已获得最新的 DNS 和 WINS 服务器 IPv4 地址列表，应手动配置路由和远程访问的 DHCP 中转代理组件，而不是依赖 VPN 服务器使用自己的 DNS 和 WINS 服务器 IPv4 地址配置 VPN 客户端。

2. 路由到 Internet 和内网的 VPN 服务器

VPN 服务器可以看作一台特殊的 IP 路由器，负责转发 VPN 客户端和内网节点之间的数据包。所以必须使用可以到达 Internet 和内网任意位置的路由器设置来进行配置。对于 IP 通信而言，VPN 服务器需要满

足如下要求。

- 默认路由：指向防火墙或直接连接 Internet 的路由器，以便使其可以到达 Internet 上的所有位置。
- 一条或多条路由：可以概括内网中使用的地址，并且指向临近内网的路由器，使 VPN 服务器可以到达所有内网的位置。

对于指向 Internet 的默认路由，使用默认网关配置 VPN 服务器的 Internet 接口，但是不使用默认网关配置内网接口。如果使用默认网关配置内网接口，则用户将会在 VPN 服务器的 IPv4 和 IPv6 路由表中拥有多个默认路由。由于 TCP/IP 协议选择默认路由转发默认路由通讯的方式，拥有多个默认路由将导致默认路由通讯被转发到内网，使得 Internet 位置不可到达。

为了添加内网路由到 VPN 服务器的路由表中，应完成如下工作。

- 使用“路由和远程访问”管理单元添加 IP 静态路由。用户不必为内网中的每个子网都添加路由。通常情况下，只需要添加能够涵盖内网所使用的 IPv4 或 IPv6 地址的路由即可。
- 如果在内网中使用路由消息协议(RIP)，则用户可以添加和配置路由和远程访问服务的 RIP 组件，从而保证 VPN 服务器作为 RIP 路由器参与到内网路由消息传播中。



提示：上述说明是针对内网中包含多个子网或 VLAN 的情况而言的。如果内网中只有一个子网，则不需要更多的配置。

3. 路由到内网的 VPN 客户端

从内网到 VPN 客户端的可到达性取决于如何配置 VPN 服务器使其获取 IP 地址，并分配给 VPN 客户端。分配给 VPN 客户端的 IPv4 地址可以是如下模式之一。

- On-subnet address range：VPN 服务器所属内网子网的地址范围。
- Off-subnet address range：VPN 服务器逻辑所属的不同子网的地址范围。

如果使用 On-subnet address range 模式，则不需要配置其他路由，因为 VPN 服务器可以作为到达 VPN 客户端的所有数据包的 ARP 代理。在 VPN 服务器子网的路由器和主机转发数据包到 VPN 客户端，再到 VPN 服务器。

如果使用 Off-subnet address range 模式，则必须在子网路由基础结构中，添加概括子网地址范围的路由，保证 VPN 客户端的通讯被转发到 VPN 服务器，然后从 VPN 服务器到 VPN 客户端。为了提供路由地址范围的最好概括，可以选择使用单一前缀和子网掩码表示的地址范围。

为了添加涵盖子网地址范围的路由到内网的路由基础结构中，需添加静态路由到 VPN 服务器的相邻路由器中，配置相邻路由器传播该静态路由到使用动态路由协议的其他路由器上。

如果内网包含单独的子网，用户必须为子网地址范围的持续路由配置每个内网主机，或者使用 VPN 服务器作为默认网关配置每个内网主机。所以，对于包含单独子网的 SOHO 网络推荐使用 On-subnet address range 池。

对基于 IPv6 的 VPN 连接，分配给路由器广播消息中的 VPN 客户端的子网前缀总是属于独立于 VPN 服务器连接的子网。所有分配了相同子网前缀的 VPN 客户端，通常都是使用 Off-subnet address range。为了从内网可到达 VPN 客户端，用户必须添加子网前缀作为指向 VPN 服务器的路由。

4. 内网路由基础结构的要求

VPN 服务器连接的内网路由结构应满足如下要求。

- 使用默认网关配置 VPN 服务器的 Internet 接口，但不要使用默认网关配置 VPN 服务器的内网接口。
- 添加概括内网地址的 IPv4 和 IPv6 路由到 VPN 服务器上。如果用户为 IPv4 动态路由协议使用 RIP，则配置和启用 VPN 服务器上的 RIP 即可；如果用户使用路由协议而非 RIP，那么可能要使用路由重新分配。
- 为 VPN 客户端添加 IPv6 子网前缀到 IPv6 路由基础结构中，作为指向 VPN 服务器的路由。



提示：推荐使用 On-subnet address range 配置 VPN 服务器，通过 DHCP 获取 IPv4 地址或者手动配置 On-subnet 地址池。

11.2.6 VPN 客户端的内网和 Internet 并存访问

默认情况下，当基于 Windows 的 VPN 客户端建立 VPN 连接时，会自动为 VPN 连接添加新的默认路由，并且修改现有默认路由，即断开客户端计算机到 VPN 服务器之外的所有其他 Internet 连接。为了防止创建新的默认路由，用户可以配置 VPN 连接不使用远程网络的默认网关。

① 在“控制面板”的“网络连接”窗口中，右击 VPN 网络连接并选择“属性”命令，打开“VPN 连接 属性”对话框，切换到“网络”选项卡，双击“Internet 协议版本 (TCP/IPv4)”项目，弹出“Internet 协议版本 4(TCP/IPv4) 属性”对话框，如图 11-2 所示。

② 单击“高级”按钮，显示“高级 TCP/IP 设置”对话框。切换到“IP 设置”选项卡，取消选中“在远程网络上使用默认网关”复选框即可，如图 11-3 所示。

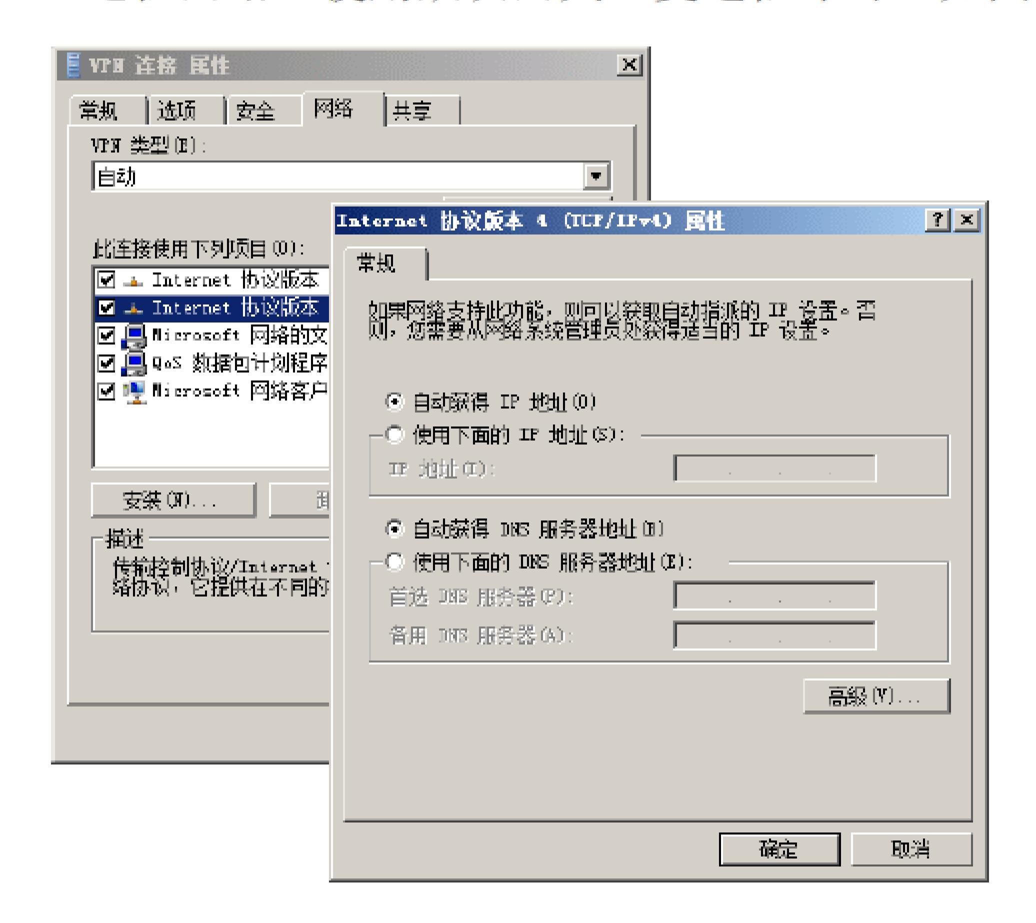


图 11-2 “Internet 协议版本 4(TCP/IPv4) 属性”对话框

图 11-3 “高级 TCP/IP 设置”对话框

经过上述设置后，在建立连接时将不会创建默认路由。但是，符合分配 IPv4 地址的 Internet 地址类的路由将会被创建。例如，如果分配的地址为 10.0.12.119，那么基于 Windows 的 VPN 客户端会使用子网掩码 255.0.0.0 为地址前缀 10.0.0.0 创建路由。

“在远程网络上使用默认网关”选项的功能如下。

- 如果取消选中此复选框，则客户端计算机连接到 VPN 服务器时仍可以访问 Internet，除了符合分配 IP 地址地址类可以到达内网，其他的则不可到达内网。

- 如果选中此复选框，则所有内网位置都可到达，除了 VPN 服务器的地址和通过其他路由的可以到达 Internet，其他的则不可到达 Internet。

对于大部分连接 Internet 的 VPN 客户端，这种行为不能说明问题，因为它们通常参与内网或 Internet，而不是参与这两者。因此，系统默认选中“在远程网络上使用默认网关”复选框。对于需要并存访问内网和 Internet 资源的 VPN 客户端，用户可以完成如下操作之一。

- 选中“在远程网络上使用默认网关”复选框，并且允许通过企业内网访问 Internet。在 VPN 客户端和 Internet 主机之间的 Internet 通讯将会穿过防火墙或代理服务器。尽管在性能上会有所影响，但是当 VPN 客户端连接着企业网络时，这种方式允许 Internet 访问被筛选，并且根据企业网络策略进行监视。
- 如果内网中的 IPv4 寻址是根据单一分类的地址前缀，则可以取消选中“在远程网络上使用默认网关”复选框。
- 如果内网中的 IPv4 寻址不是根据单一分类的地址前缀，则用户可以使用如下解决方式。
  - 无等级静态路由 DHCP 选项。
  - 连接管理工具。
  - 在 VPN 客户端上的命令文件。

11.2.7 身份验证基础结构

身份验证是贯穿整个 VPN 连接的重要操作，主要分布于 VPN 服务器、专业 RADIUS 认证服务器、域控制器、证书颁发机构(CA)等。

1. Windows 身份验证

基于 Windows Server 2008 的 VPN 服务器可以配置使用 Windows 或 RADIUS 来进行身份验证或记账。当 VPN 服务器使用 Windows 进行身份验证时，通过与域控制器通信执行 VPN 连接的身份验证。当 VPN 服务器使用 RADIUS 进行身份验证时，依靠 RADIUS 服务器执行身份验证和授权。

当 VPN 服务器使用 Windows 进行身份验证时，根据在“网络策略服务器”管理单元中的“记账”节点的设置，记录 VPN 连接信息在本地日志文件中(默认情况下为%SystemRoot%\System32\Logfiles\Logfile.log)。当 VPN 服务器使用 RADIUS 进行身份验证时，依靠 RADIUS 服务器记录记账信息。

2. RADIUS 身份验证服务器

当用户拥有多个 VPN 服务器或者其他类型访问服务器，则可以使用 RADIUS 提供集中身份验证、授权和记账服务。

如果使用 RADIUS 和 Windows 域作为用户账户数据库，验证用户证书和获取拨号属性，那么用户应该使用 Windows Server 2008 中的 NPS。NPS 是一种全功能的 RADIUS 服务器和代理，可与活动目录和路由与远程访问相结合。

当 NPS 作为 RADIUS 服务器使用时，可完成如下工作。

- NPS 通过与域控制器通信来执行 VPN 连接的身份验证。NPS 通过 NPS 服务器上的用户账户和网络策略的拨号属性来执行连接尝试的授权。
- 默认情况下，NPS 根据在“网络策略服务器”管理单元中的“记账”节点的设置，记录所有 RADIUS 记账信息在本地日志文件中(默认情况下为%SystemRoot%\System32\Logfiles\Logfile.log)。

11.2.8 VPN 客户端

VPN 客户端可以是使用 MPPE(微软点对点加密协议)加密创建 PPTP 连接的计算机，也可以是使用 IPSec 加密创建 L2TP 连接的计算机，还可以是使用 SSL 加密创建 SSTP 连接的计算机。运行 Windows Vista、Windows Server 2008、Windows Server 2003 或 Windows XP 的 VPN 客户端可以创建 PPTP 或基于 L2TP/IPSec 的 VPN 连接。运行 Windows Vista SP1 或 Windows Server 2008 的 VPN 客户端可以创建基于 SSTP 的 VPN 连接。用户可以手动配置或者通过使用 Windows Server 2008 的连接管理器组件来配置 VPN 客户端的 VPN 连接。

1. 连接管理器

Windows Server 2008 系统集成的连接管理器组件(CM)，可以大大简化 VPN 客户端的配置过程，适用于 IT 专业人员。连接管理器包含如下组件。

- 连接管理器客户端拨号盘。
- 连接管理器工具。
- 连接点服务。

(1) 连接管理器客户端拨号盘

连接管理器客户端拨号盘是安装在每个 VPN 客户端上的软件，它包含的高级功能使其成为基本远程访问网络的扩展。同时，CM 客户端拨号盘为用户简化了连接过程。它限制了用户可以更改的配置选项数量，确保用户可以总是连接成功。例如，CM 客户端拨号盘可以完成如下操作。

- 使用定制图表、符号、信息和帮助。
- 在 VPN 连接建立之前自动创建拨号连接。
- 在各种连接过程中运行常用动作。
- 对于拨号连接，从使用的电话号码列表中根据物理位置选择。

定制的 CM 客户端拨号盘配置文件，是由网络管理员使用连接管理工具(CMAK)创建的可执行文件。CM 配置文件通过 CD-ROM、E-mail、Web 站点或文件共享分布于 VPN 用户。当用户运行 CM 配置文件时，它会自动配置定制拨号或 VPN 连接。CM 配置文件不需要指定 Windows 的版本，适用于 Windows Vista、Windows Server 2008、Windows Server 2003 或 Windows XP 的计算机配置连接。

(2) 连接管理工具

用户可以通过使用 CMAK 来创建定制 CM 配置文件。使用 CMAK，用户可以配置客户端拨号软件，通过使用指定连接功能来允许用户连接网络。CM 配置文件支持多种功能，包含简化和加强版的连接执行。CMAK 允许用户建立 CM 配置文件，定制 CM 客户端拨号盘，以保证连接反映企业的个性。

(3) 连接点服务

对于拨号 CM 配置文件，连接点服务(CPS)允许用户自动分配和更新电话簿。这些电话簿包含一个或多个到场点(POP)条目，每个 POP 都提供一个电话号码对内网拨号访问，或者访问 Internet 访问点。电话簿为用户提供完整的 POP 信息，保证用户旅行时可以连接不同的 Internet 访问点。

如果没有自动更新电话簿的能力，用户将会需要联系企业的技术支持，更改 POP 信息，并且重新配置客户端拨号盘软件。

CPS 包含如下两个组件。

- 电话簿管理员：一种创建和维护电话簿数据库，并发布新的电话簿信息到电话簿服务的工具。
- 电话簿服务：IIS 7.0 的扩展。CM 配置文件可以配置用来检查在指定 IIS 服务器上运行的电话簿服务，确保使用最新的电话簿，否则，远程访问客户端会自动下载电话簿更新。

2. VPN 客户端的设计原则

部署 VPN 客户端时应遵循如下原则。

- 如果 VPN 客户端数量较少，则可以在每台计算机上执行 VPN 连接的手动配置。
- 如果 VPN 客户端数量较多，或者分别运行着不同 Windows 版本，则建议使用 Windows Server 2008 的 CM 组件创建包含 VPN 配置设置的 CM 配置文件，并且对于拨号连接，需要维护电话簿数据库。
- 对于 L2TP/IPSec 连接，用户必须在 VPN 客户端计算机上安装计算机证书。
- 对于 PEAP-TLS 或 EAP-TLS 身份验证方式，必须在 VPN 客户端上安装用户证书，或者为用户发布智能卡。
- 对于 SSTP 连接，用户必须确保 VPN 客户端安装了 VPN 服务器的计算机证书的发布 CA 的根 CA 证书。
- 对于 PEAP-MS-CHAP v2 或 PEAP-TLS 身份验证方式，如果 VPN 客户端验证了认证服务器的证书(推荐)，那么用户必须确保 VPN 客户端安装了身份验证服务器的计算机证书的发布 CA 的根 CA 证书。

11.2.9　PKI

PKI(Public Key Infrastructure，公钥基础设施)是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务具有普遍性的安全基础设施。在 VPN 连接中，可以为 L2TP 连接指定基于证书的身份验证，为使用 PEAP-TLS 或 EAP-TLS 的 VPN 连接执行智能卡或用户证书身份验证。对于基于 PEAP-MS-CHAP v2 的身份验证和基于 SSTP 的 VPN 连接，不需要 PKI，可以从第三方证书颁发机构获得证书，安装在身份验证服务器或 VPN 服务器上。用户也可能需要分配第三方计算机证书的根 CA 和中间 CA 证书给 VPN 客户端计算机。

1. L2TP/IPSec 连接的计算机证书

当用户为 L2TP/IPSec 连接使用证书身份验证方式时，证书颁发机构(CA)的列表是不可配置的。每个 IPSec 端从接收证书身份验证的地方发送根 CA 的列表，列表中的根 CA 与发布计算机证书的根 CA 相符合。例如，如果计算机 A 通过根 CA CerAuth1 和 CerAuth2 来发布计算机证书，则它会通知 IPSec 端只能从 CerAuth1 和 CerAuth2 处接收身份验证证书；如果计算机 B 没有有效的计算机证书，IPSec 协商将会失败。

VPN 客户端必须安装了有效的计算机证书，该证书由 VPN 服务器信任的根 CA 的证书链中的 CA 发布。此外，VPN 服务器必须安装了 VPN 客户端信任的根 CA 的证书链中的 CA 发布的计算机证书。

企业通常拥有单一根 CA 和一个或多个发布计算机证书的根 CA 的发布 CA。由于此原因，企业中的所有计算机必须拥有证书链 CA 发布的有效的计算机证书，以及相同单一根 CA 的发布 CA 的请求证书。

2. 智能卡的 PKI

智能卡的使用是 Windows Server 2008 中用户身份验证最安全的方式。对于远程访问 VPN 连接，用户可以使用带有 EAP-TLS 或 PEAP-TLS 身份验证方式的智能卡。个人智能卡分配的用户需要在计算机上拥有

智能卡读卡器。登录计算机时，需要将智能卡插入读卡器中，并输入智能卡个人识别码。

3. 用户证书的 PKI

当用户具有智能卡并且指定使用个人识别码登录计算机时，Windows 系统中用于用户身份验证的用户证书可以代替智能卡，不过这种方式的安全性较低。

11.2.10 NAP 的 VPN 强制

Windows Server 2008、Windows Vista 和 Windows XP SP3 系统中的网络访问保护(NAP)组件，可以帮助用户强制网络访问或通信的健康策略的符合性。管理员可以创建验证计算机的解决方案，提供更新或访问必要的资源，并且限制不符合的计算机访问网络。

VPN 强制是 NAP 强制方式的一种。使用 VPN 强制，在允许完全访问内网之前，远程访问客户端必须与系统健康要求相符合。如果 VPN 客户端与系统健康要求不符合，则只能访问受限网络，其中包含可以将 VPN 客户端更新为符合健康策略的修补服务器。VPN 服务器通过 IP 数据包筛选器来强制受限访问。在更正了健康状态之后，VPN 客户端再次验证健康状态，如果符合，则限制访问的 IP 数据包筛选器将被删除。

VPN 强制操作仅适用于基于 Windows Server 2008 的 VPN 服务器，并且使用基于 PEAP 的身份验证方式。

11.3 配置基于 VPN 的远程访问

一个基本的 VPN 远程连接应包含 3 个基本部分，即 VPN 服务器、身份验证机构和 VPN 客户端。其中，VPN 服务器和 VPN 客户端是必不可少的，而身份验证方式是确保远程连接安全的重要手段，如数字证书、Windows 身份验证、RADIUS 身份验证等。为了便于和网络中的其他服务器协同工作，建议在域中部署 VPN 服务器和其他身份验证服务器。

11.3.1 配置证书

数字证书是确保 VPN 安全连接和传输的重要元素。用户可以将数字证书颁发机构(CA)部署在 VPN 服务器或域控制器上，也可以单独部署。但是，如果 VPN 和 CA 共用一台服务器，偶尔会产生无法颁发证书的错误，因此，建议在域控制器上部署 CA。数字证书和 VPN 支持的加密协议协同工作，可实现如下安全功能。

- 结合数字证书的 L2TP/IPSec 加密连接。用户必须为每台 VPN 客户端计算机和 VPN 服务器准备所需的计算机证书。需要注意的是，L2TP/IPSec 连接的预共享密钥身份验证是一种较不安全的认证方式，不推荐使用。
- 使用智能卡或用户证书的 EAP-TLS 或 PEAP-TLS 的身份验证。用户必须为每台 VPN 客户端准备智能卡或用户证书，每台认证服务器都需要计算机证书。
- PEAP-MS-CHAP v2 身份验证。每台认证服务器都需要计算机证书，并且每台 VPN 客户端都需要安装认证服务器的计算机证书的证书链。
- SSTP 安全。用户必须为 VPN 服务器准备证书，并且为每台 VPN 客户端准备 VPN 服务器计算机证书的发布 CA 的根 CA 证书。

1. 配置计算机证书

CA 的安装过程比较简单，这里不作详细介绍。本例中将 CA 部署在域控制器上，VPN 连接中应用的所有计算机证书和用户账户证书，均由此 CA 颁发。通常情况下，管理员可以使用如下方式在 VPN 客户端、VPN 服务器或认证服务器上安装计算机证书。

- 为活动目录域的计算机配置计算机证书的自动注册。
- 使用“证书”管理单元请求计算机证书。
- 使用“证书”管理单元导入计算机证书。
- 通过 Web 申请证书。
- 执行 CAPICOM 脚本申请计算机证书。

2. 配置根 CA 证书

如果用户正在使用 PEAP-MS-CHAP v2 身份验证或 SSTP 加密连接，则还需要配置根 CA 证书。

如果用户使用 PEAP-MS-CHAP v2 身份验证方式，则可能需要在 VPN 客户端上安装认证服务器所使用的计算机证书的根 CA 证书。如果认证服务器所使用的计算机证书的根 CA 证书已经安装在 VPN 客户端上，则不需要其他配置。

如果用户使用 SSTP 连接，那么可能需要安装 VPN 服务器所使用的计算机证书的根 CA 证书。如果 VPN 服务器所使用的计算机证书的根 CA 证书已经安装在 VPN 客户端上，那么就不需要其他的配置了。

确认 VPN 服务器和客户端均已安装根 CA 证书，即同时信任此证书颁发机构。在 VPN 服务器上，使用计算机证书管理控制台，查看是否已经获得证书服务器的根 CA 证书，并安装在“受信任的根证书颁发机构”中，如图 11-4 所示。

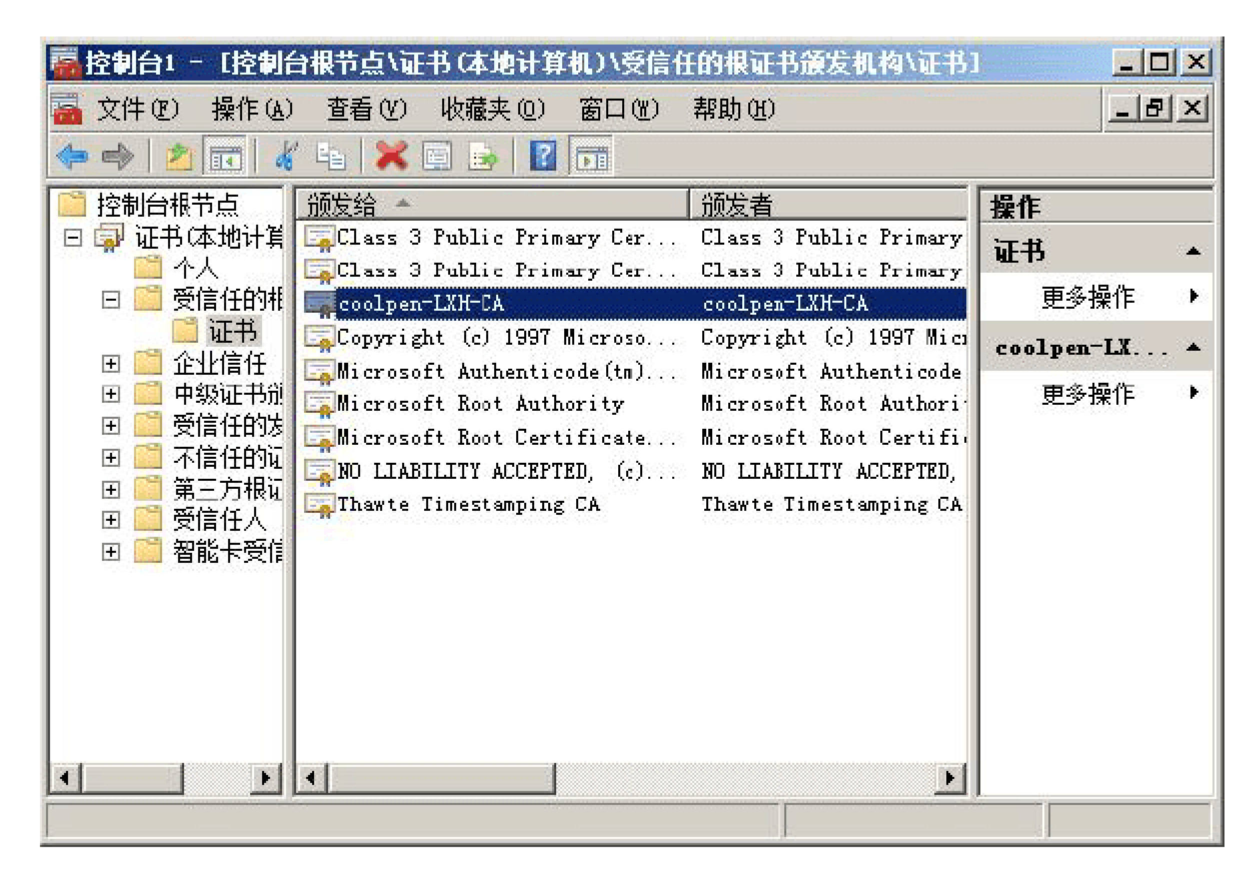


图 11-4　检查 VPN 服务器上的根 CA 证书

VPN 客户端同样需要安装证书服务器的根 CA 证书，确认方法与 VPN 服务器完全相同，这里不复赘述。

3. 配置用户证书

用户账户证书主要用于确认拨入 VPN 服务器时使用的用户账户的有效性，获取方式与计算机证书完全相同，此处不复赘述。需要注意的是，客户端验证是否获取证书时，需要在 MMC 控制台中添加“用户账户”证书控制台，与计算机证书略有不同。

11.3.2 配置 Internet 基础结构

在配置远程访问服务器之前，应事先做好 Internet 基础结构的准备工作，例如加入域、安装并配置 DHCP 服务器等。同时，远程访问服务器上需要安装两块网卡，一块网卡设置内网地址，用来连接局域网；另一块设置公网地址，用来连接 Internet。

1. 设置 IP 地址

VPN 服务器需要安装两块网卡，一块连接局域网；另一块用来连接 Internet，供远程用户拨入局域网。为连接局域网的本地连接设置局域网 IP 地址，如图 11-5 所示。DNS 服务器设置为域控制器的 IP 地址，用来加入域。

将另一个连接 Internet 的本地连接的 IP 地址设置为 Internet 上有效的 IP 地址，如图 11-6 所示。

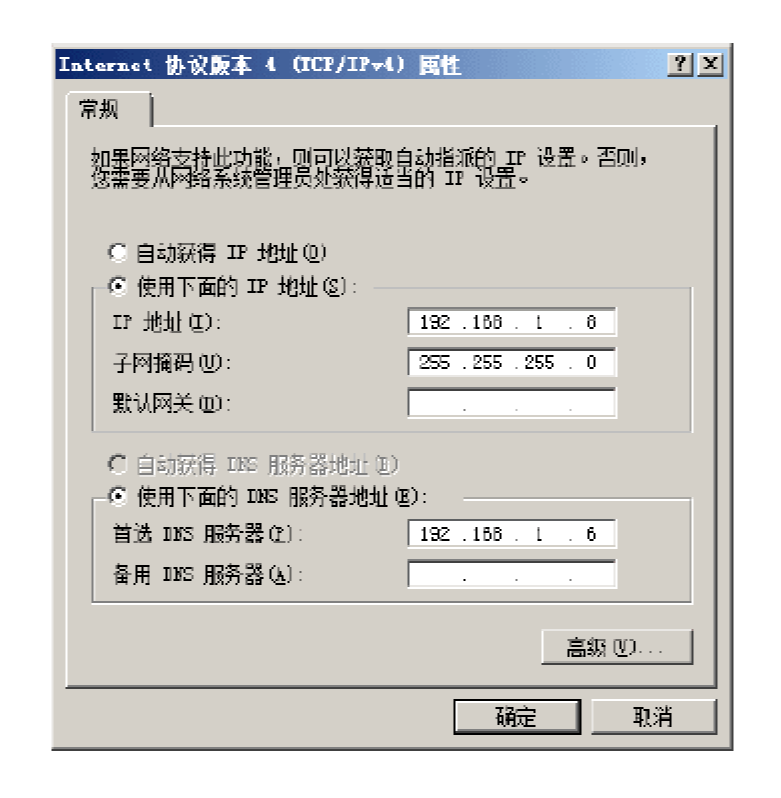


图 11-5 设置内网 IP 地址

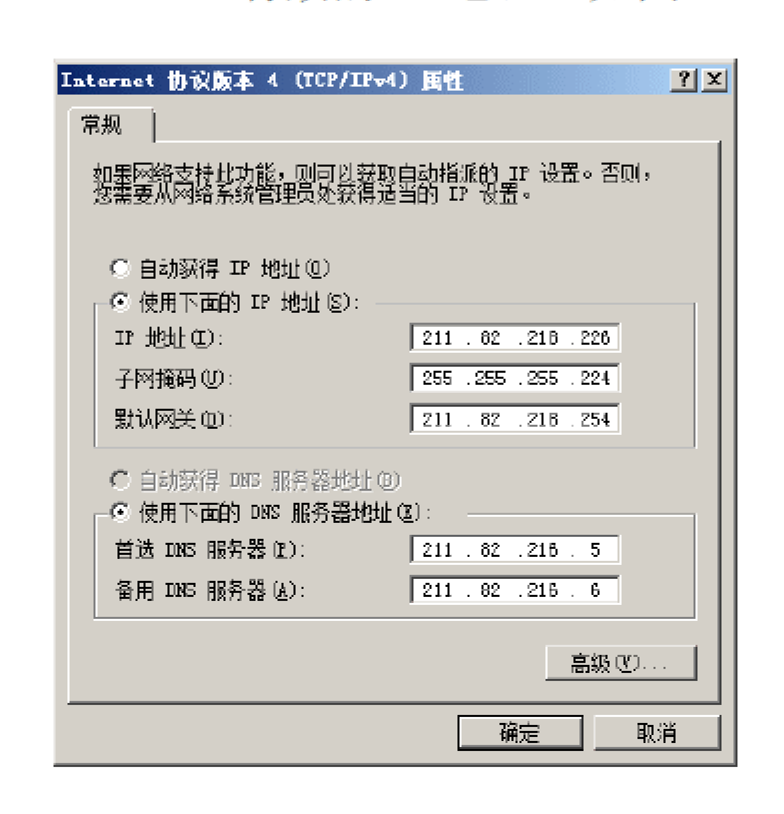


图 11-6 设置外网 IP 地址

2. 加入域

配置 VPN 远程访问之前，应将 VPN 服务器加入到域。首先将 VPN 服务器的 DNS 服务器地址指向域控制器，然后在“服务器管理器”窗口中，单击“更改系统属性”链接，打开“系统属性”对话框。切换到“计算机名”选项卡，单击“更改”按钮，弹出如图 11-7 所示的“计算机名/域更改”对话框，选择“域”单选按钮，并输入域名。单击“确定”按钮，显示“Windows 安全”对话框，在“用户名”和“密码”文本框中，输入具有加入域权限的用户名和密码即可。

单击“确定”按钮即可加入域。根据系统提示重新启动系统，使用域用户账户登录即可。

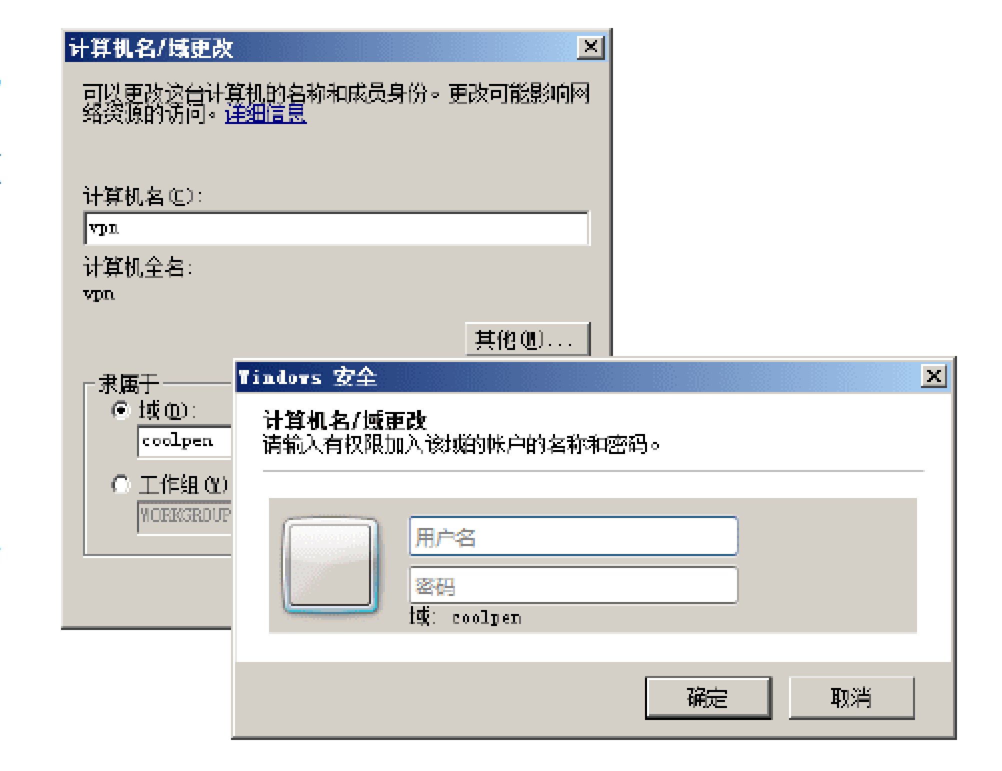


图 11-7 “计算机名/域更改”对话框

3. 安装并设置 DHCP 服务器

当远程客户端拨入局域网以后，需要获得相应的局域网 IP 地址，才能访问局域网中的资源；因此，需要在网络中部署 DHCP 服务器，创建作用域并启用网络访问保护。需要注意的是，一定要进行授权，否则无法向客户端分配 IP 地址。另外，如果不想安装 DHCP 服务

器，也可以在配置“路由和远程服务器”的过程中设置分配给客户端的 IP 地址范围。

11.3.3　赋予域用户账户远程访问权限

在域控制器上，依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口。双击希望用于 VPN 远程访问的用户账户(以 vpn 用户为例)，打开如图 11-8 所示的“vpn 属性”对话框。在“拨入”选项卡中的“网络访问权限”选项区域，选择“允许访问”单选按钮，其他选项保持默认设置。单击“确定”按钮，保存设置即可。

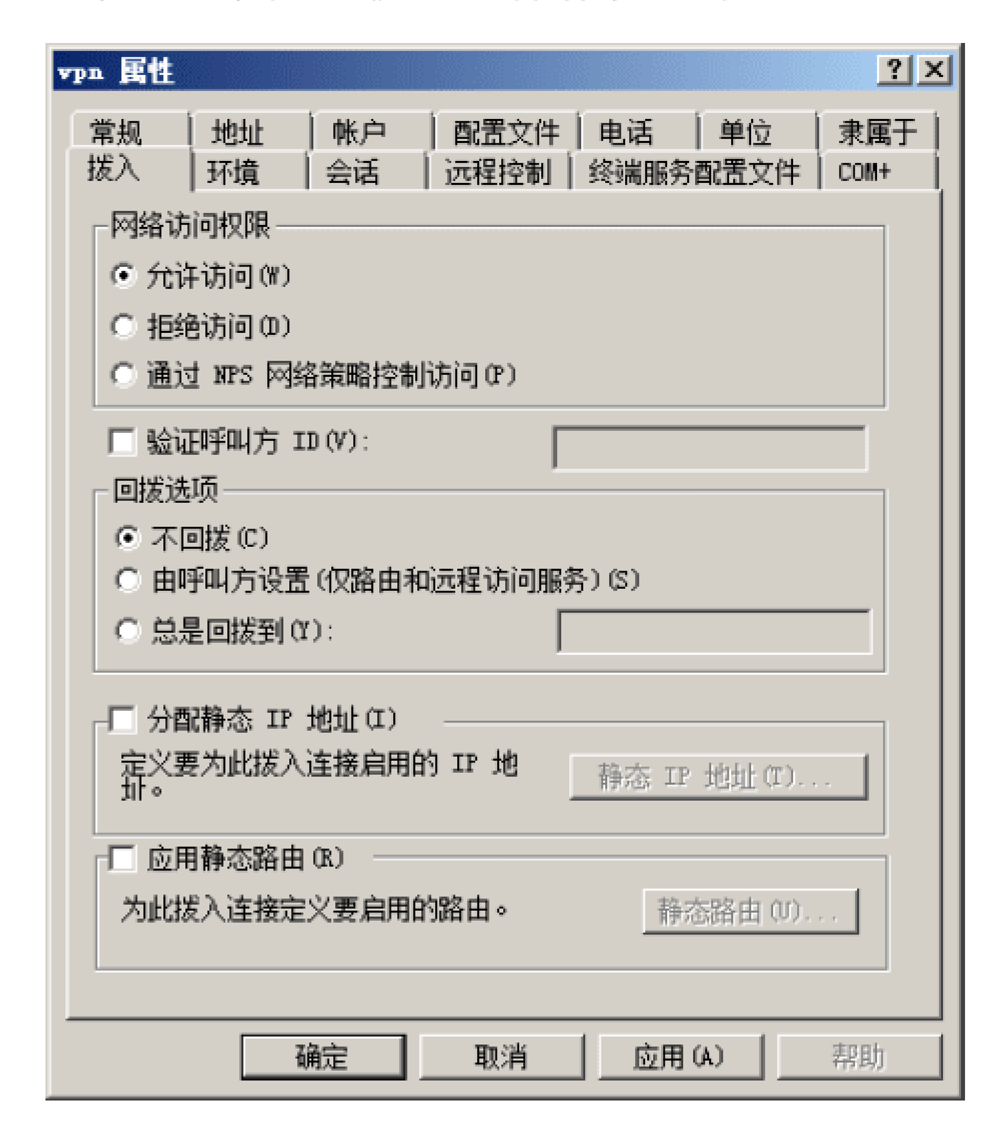


图 11-8　“vpn 属性”对话框

11.3.4　安装和配置 VPN 服务器

VPN 服务器用来提供拨入功能，供远程计算机用户拨入公司局域网。不过，VPN 服务可以与网络策略服务器配合使用，对拨入的客户端用户进行验证，只有通过网络安全验证的计算机才允许访问网络。VPN 服务器上需要安装两块网卡，一块网卡设置内网地址，用来连接局域网；另一块设置公网地址，用来连接 Internet。另外，如果希望使用 L2TP/IPSec 或 SSTP 安全连接，还必须为 VPN 服务器安装计算机证书。

1. 安装远程访问服务

① 单击“添加角色向导”链接，在打开的“选择服务器角色”界面中，选中“网络策略和访问服务”角色，如图 11-9 所示。

② 单击“下一步”按钮，显示如图 11-10 所示的“网络策略和访问服务”界面，其中显示了网络策略和访问服务的简介信息。

③ 单击“下一步”按钮，显示如图 11-11 所示的“选择角色服务”界面。由于只配置 VPN 服务器，因此，选中“路由和远程访问服务”复选框即可。



图 11-9 “选择服务器角色”界面

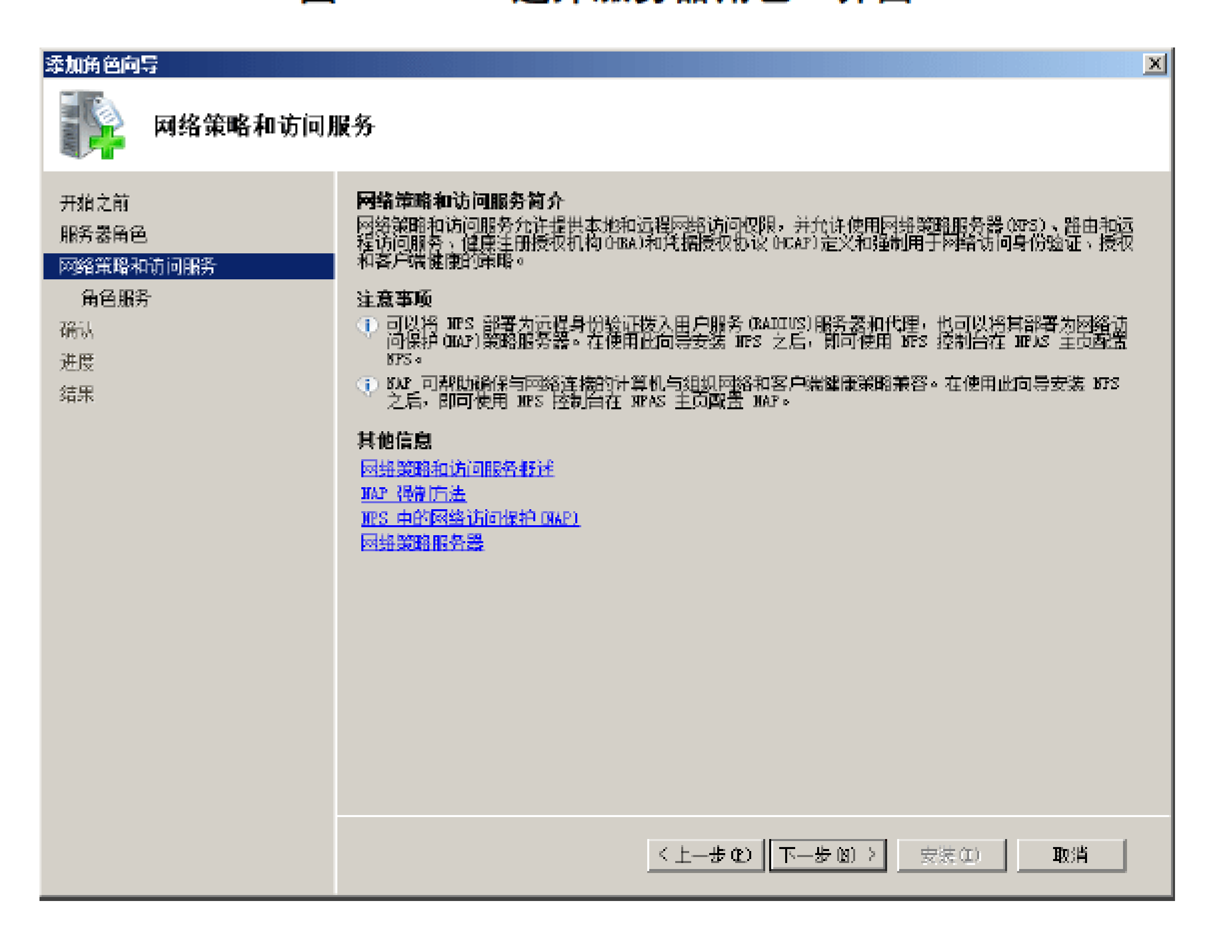


图 11-10 “网络策略和访问服务”界面

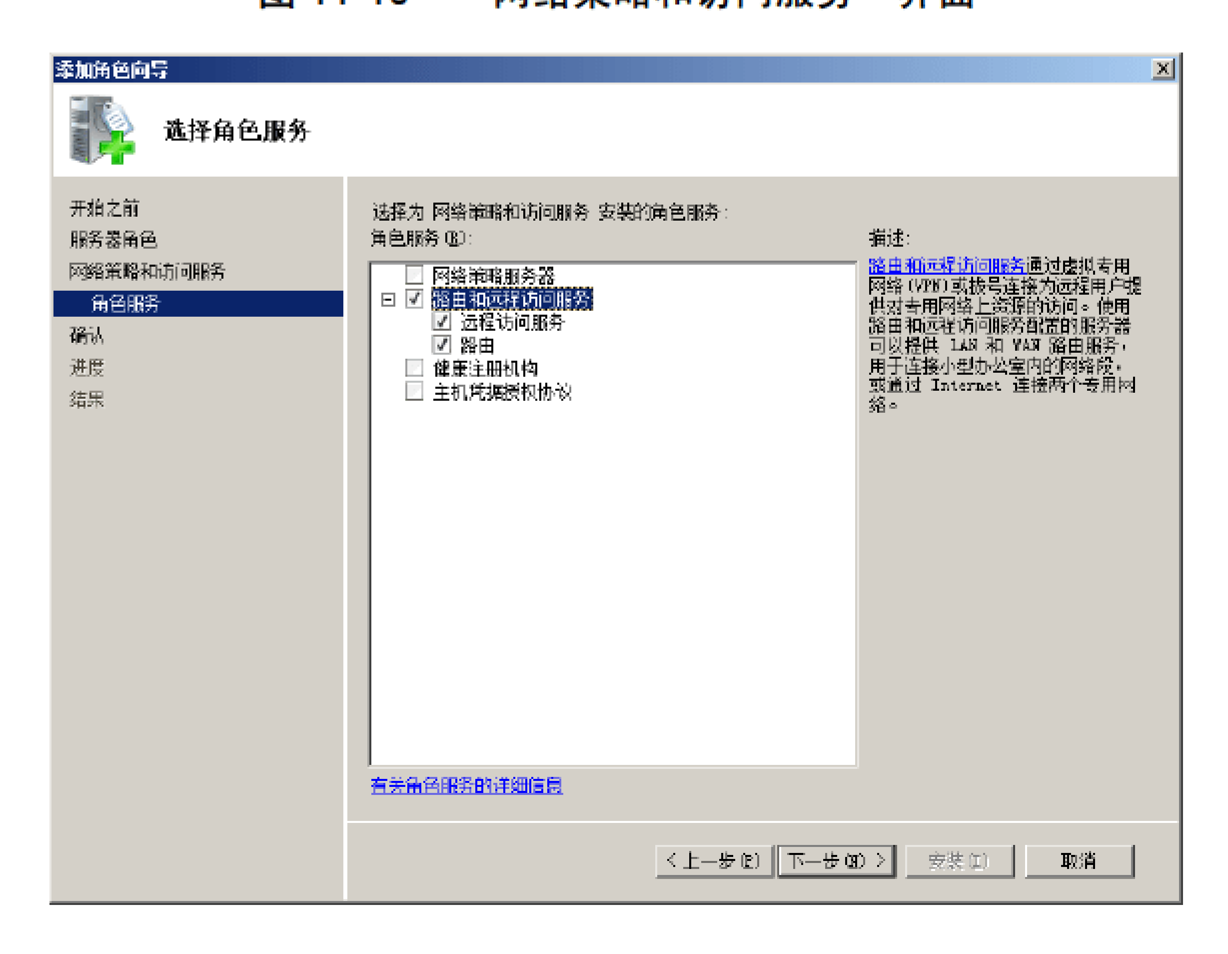


图 11-11 “选择角色服务”界面

④ 单击“下一步”按钮，显示如图 11-12 所示的“确认安装选择”界面，在此显示了将要安装的角色。

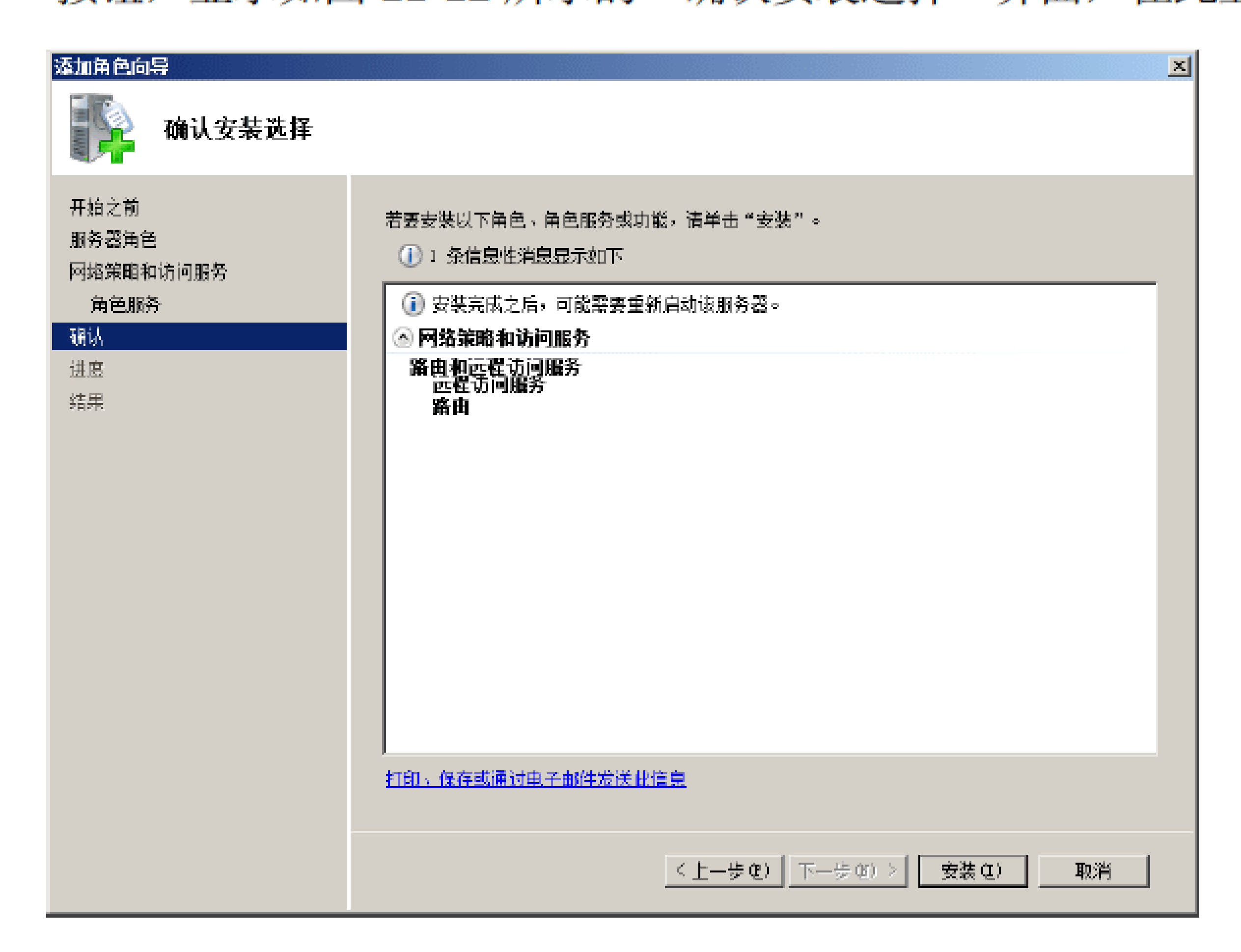


图 11-12　“确认安装选择”界面

⑤ 单击“安装”按钮，开始安装。完成后显示如图 11-13 所示的“安装结果”界面。



图 11-13　“安装结果”界面

⑥ 单击“关闭”按钮，远程访问服务安装完成。

2. 配置路由和远程访问服务

远程访问服务安装完成后，默认并没有启动，需要启用路由和远程访问功能。同时，由于 VPN 强制需要将远程拨入的用户向 NPS 服务器进行身份验证，以检查远程计算机是否符合策略要求，因此，还必须配置 RADIUS 服务器。

① 依次单击“开始”→“管理工具”→“路由和远程访问”命令，打开“路由和远程访问”控制台窗口，如图 11-14 所示，默认没有启用路由和远程访问功能。

② 右击服务器名并选择快捷菜单中的“配置并启用路由和远程访问”命令，启动“路由和远程访问服务器安装向导”，如图 11-15 所示。

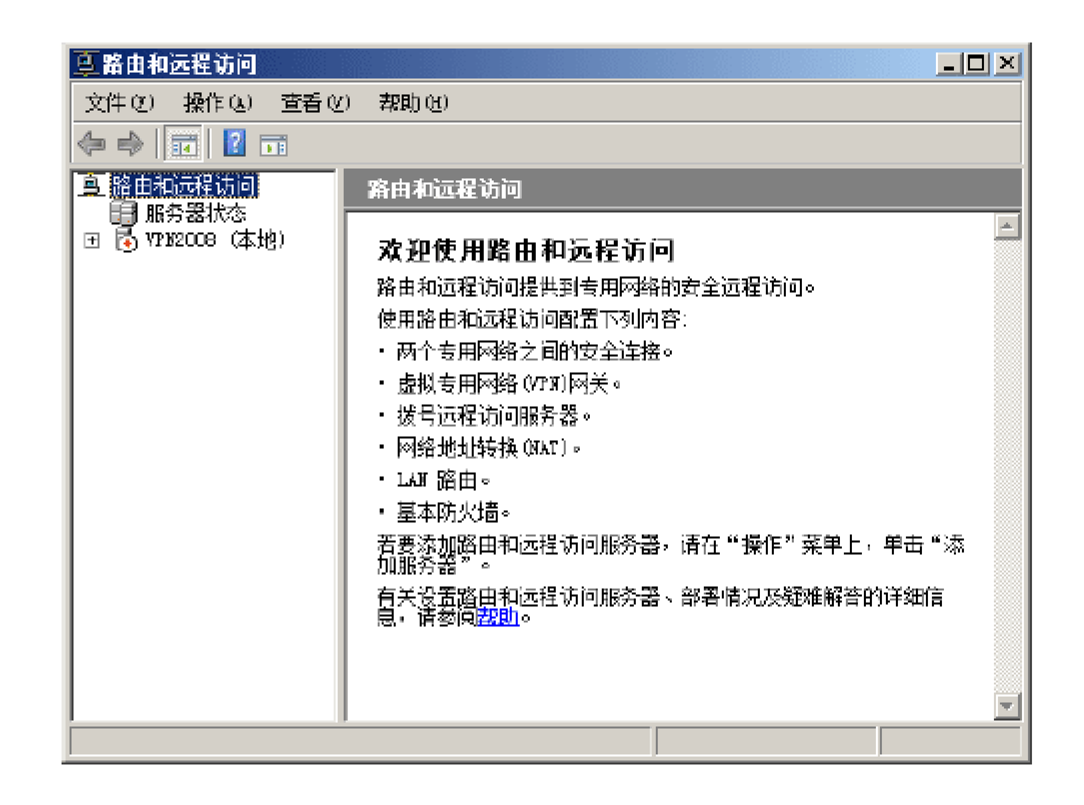


图 11-14 “路由和远程访问”窗口

图 11-15 路由和远程访问服务器安装向导

③ 单击“下一步”按钮，显示如图 11-16 所示的“配置”界面，其中提供了多种方式来实现远程访问。这里选择“远程访问(拨号或 VPN)”单选按钮。

④ 单击“下一步”按钮，显示如图 11-17 所示的“远程访问”界面。由于现在使用 VPN 连接，因此，选中 VPN 复选框，使远程客户端可以通过 Internet 利用 VPN 拨号连接到此服务器。

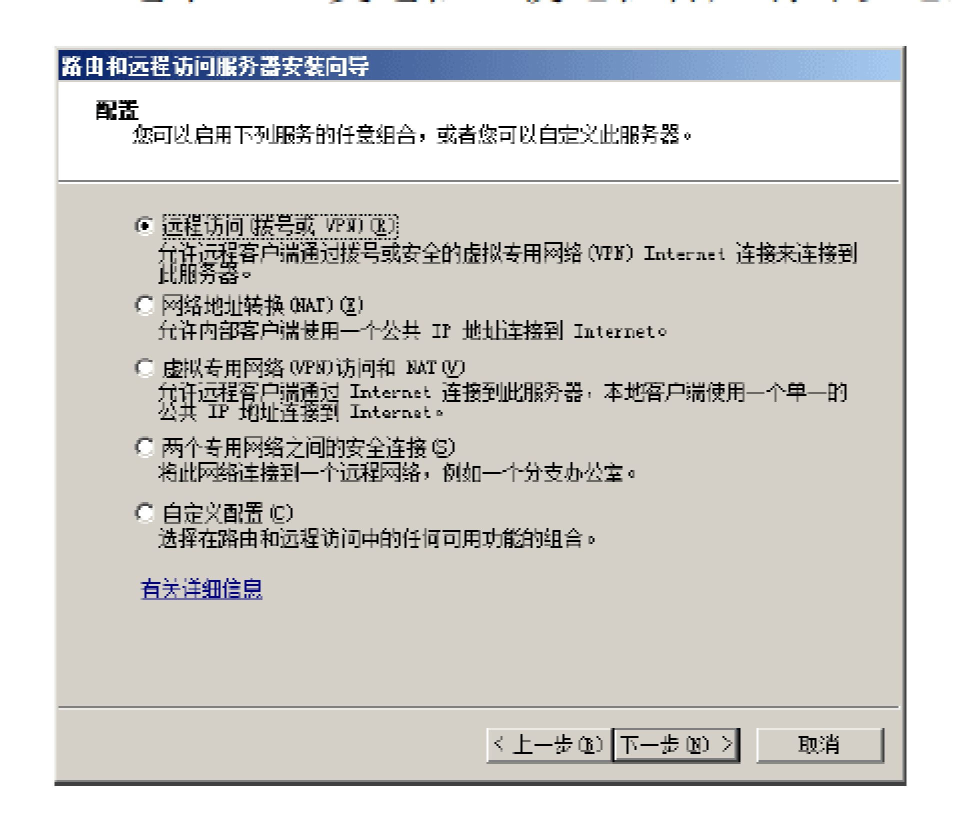


图 11-16 “配置”界面

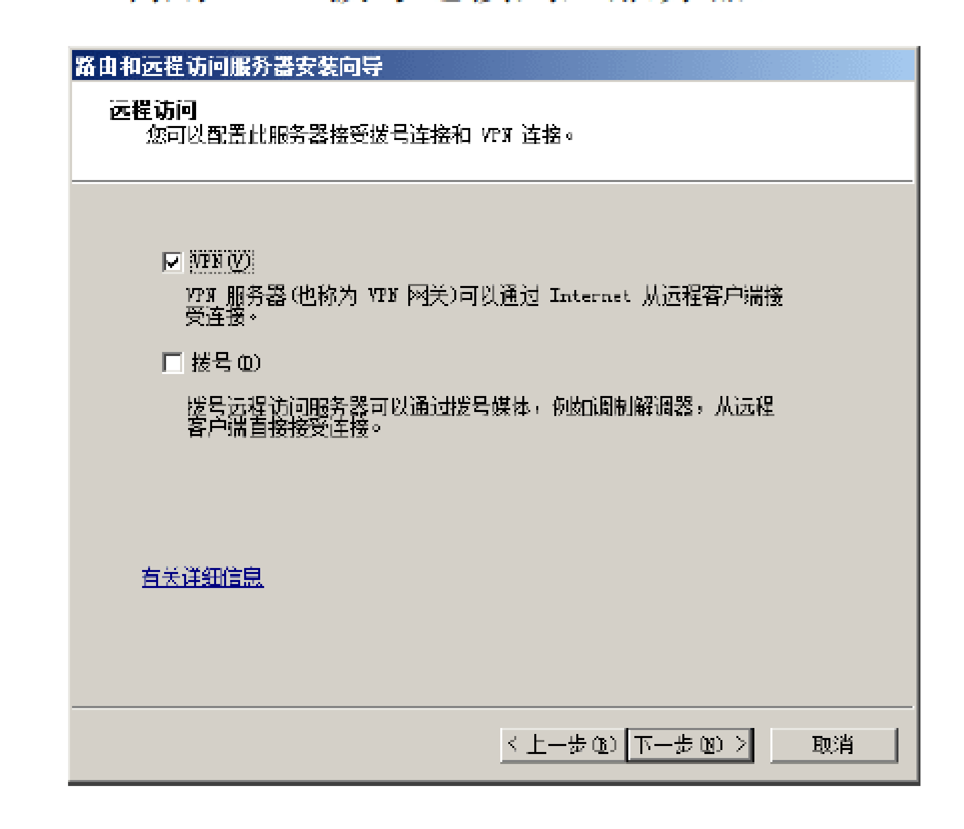


图 11-17 “远程访问”界面

⑤ 单击“下一步”按钮，显示如图 11-18 所示的“VPN 连接”界面。配置 VPN 远程访问服务器至少需要提供两块网卡，即一块连接 Internet，响应远程用户的访问；另一块用于连接内网。在“网络接口”列表框中选择此服务连接到 Internet 的连接即可。



提示： 默认选中“通过设置静态数据包筛选器来对选择的接口进行保护”复选框，只有使用 VPN 方式时，才能与所选择的本地连接通信，其他任何方式都不能通过该本地连接通信。如果 VPN 服务器需要通过该连接来连接 Internet 或其他服务器，则可取消选中该复选框。

⑥ 单击“下一步”按钮，显示如图 11-19 所示的“IP 地址分配”界面，指定远程客户端获得 IP 地址的方式。由于网络中已经配置了 DHCP 服务器，因此，选择“自动”单选按钮，使客户端自动从 DHCP 服务器获得 IP 地址即可。否则，需要选择“来自一个指定的地址范围”单选按钮并设置欲分配的 IP 范围。

⑦ 单击“下一步”按钮，显示如图 11-20 所示的“管理多个远程访问服务器”界面。由于配置 VPN

强制要求设置 RADIUS 服务器，因此，选择“是，设置此服务器与 RADIUS 服务器一起工作”单选按钮。

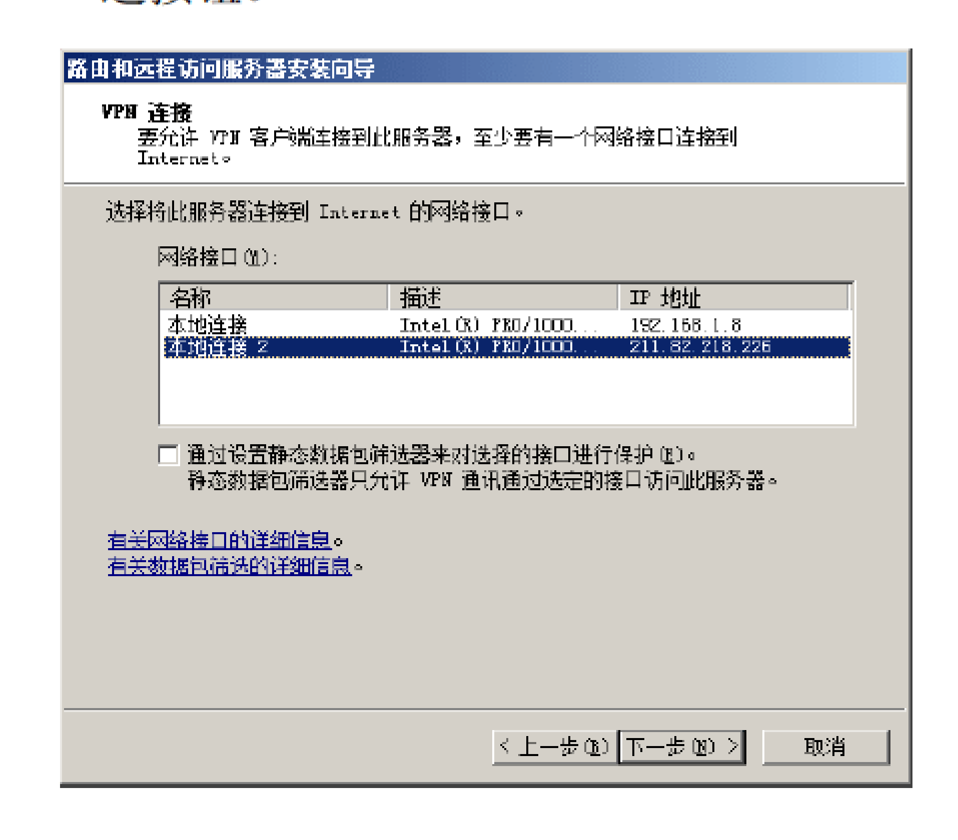


图 11-18　“VPN 连接”界面

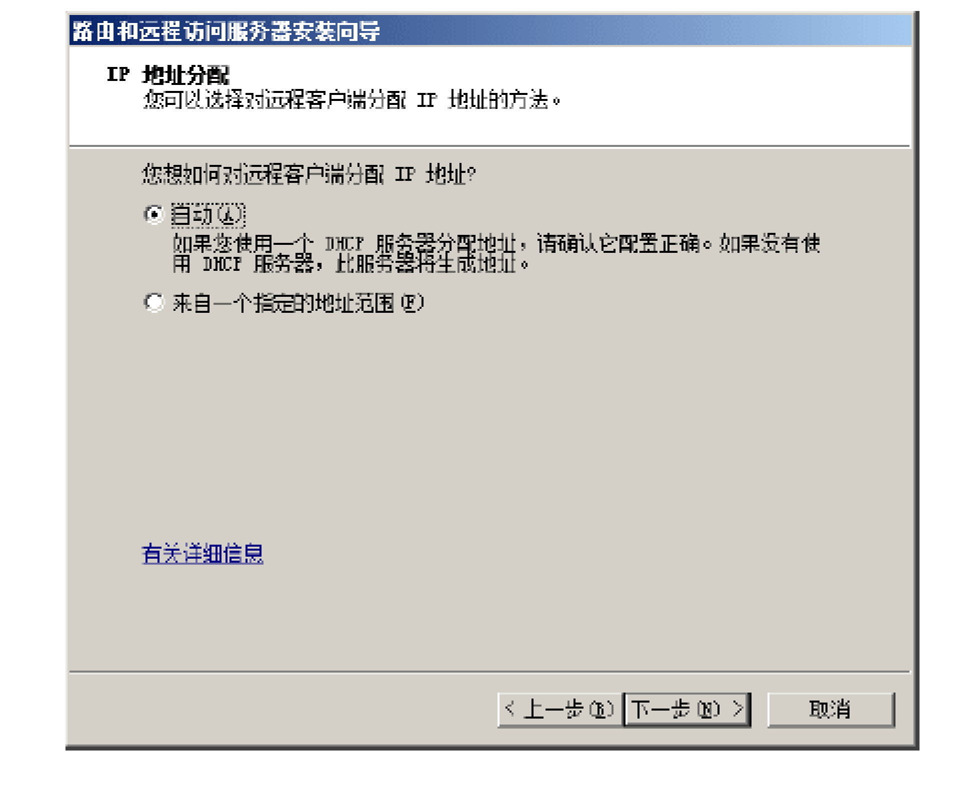
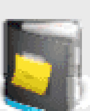


图 11-19　“IP 地址分配”界面



提示：如果仅仅提供 VPN 功能，而不使用网络访问保护功能，可选择“否，使用路由和远程访问来对连接请求进行身份验证”单选按钮。

⑧ 单击“下一步”按钮，显示如图 11-21 所示的“RADIUS 服务器选择”界面。在“主 RADIUS 服务器”文本框中，输入要为远程用户进行身份验证的 RADIUS 服务器地址。由于 NPS 服务器即是 RADIUS 服务器，因此，输入 NPS 服务器地址即可。

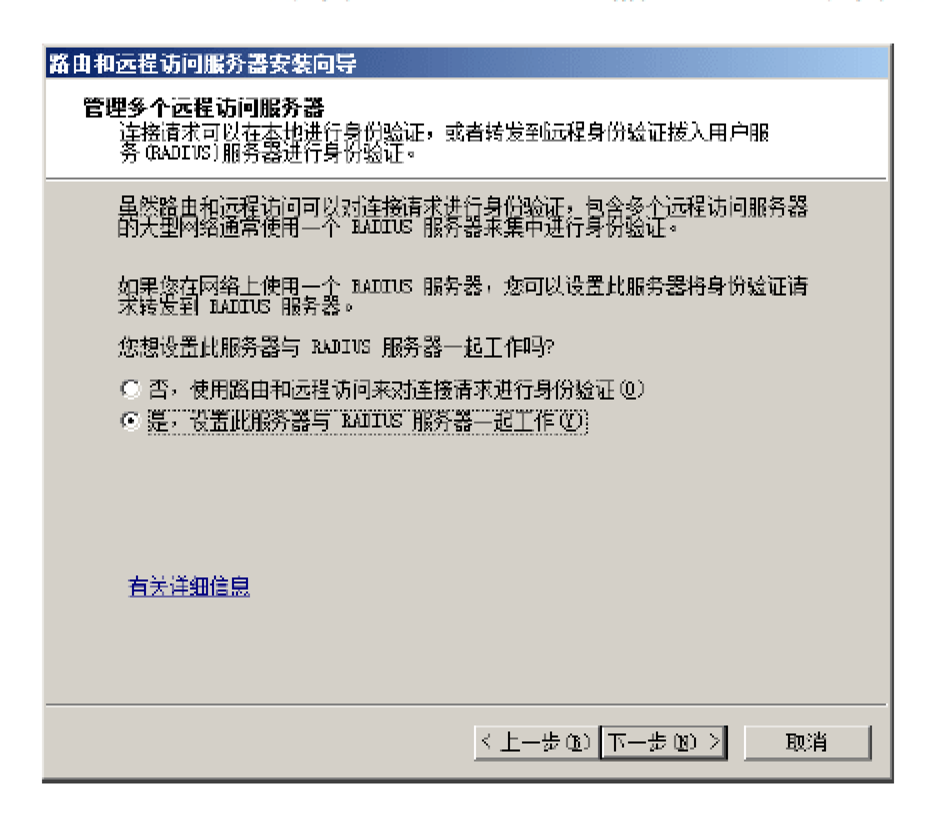


图 11-20　“管理多个远程访问服务器”界面

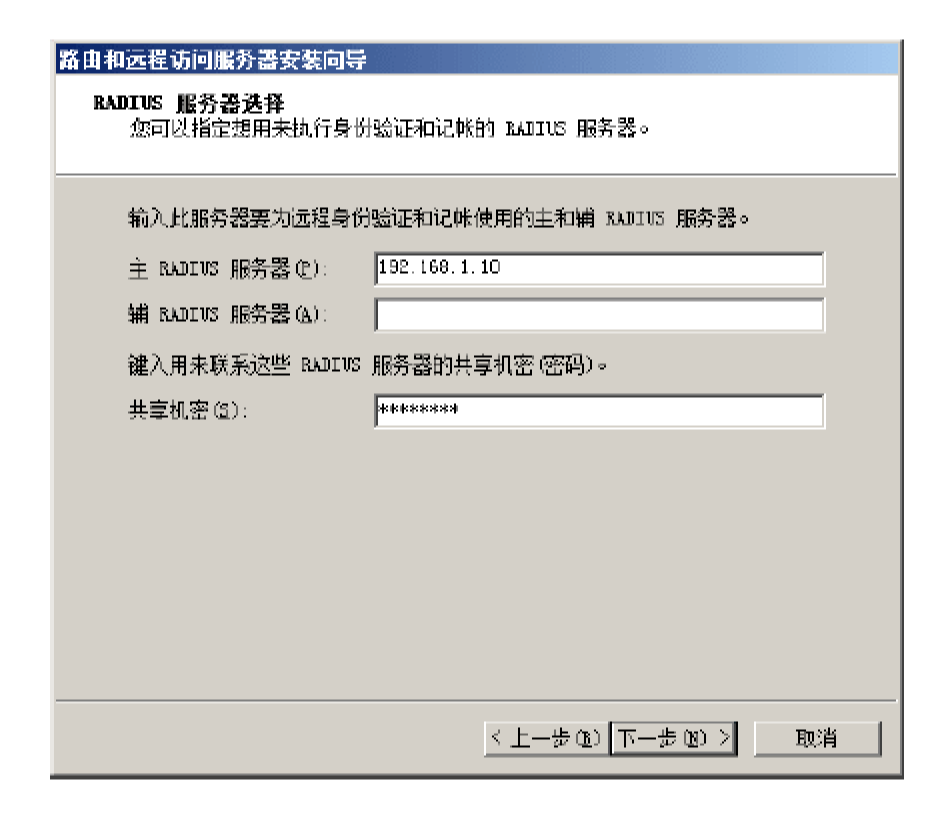


图 11-21　“RADIUS 服务器选择”界面

⑨ 单击“下一步”按钮，显示如图 11-22 所示的“正在完成路由和远程访问服务器安装向导”界面，“摘要”信息框中显示了当前所作的设置，单击“上一步”按钮可返回修改。

⑩ 单击“完成”按钮，显示如图 11-23 所示的“路由和远程访问”提示框。提示用户在设置远程访问服务器以后，需要再指定 DHCP 服务器的 IP 地址。

⑪ 单击“确定”按钮，启动路由和远程访问功能，并返回“路由和远程访问”控制台，如图 11-24 所示。

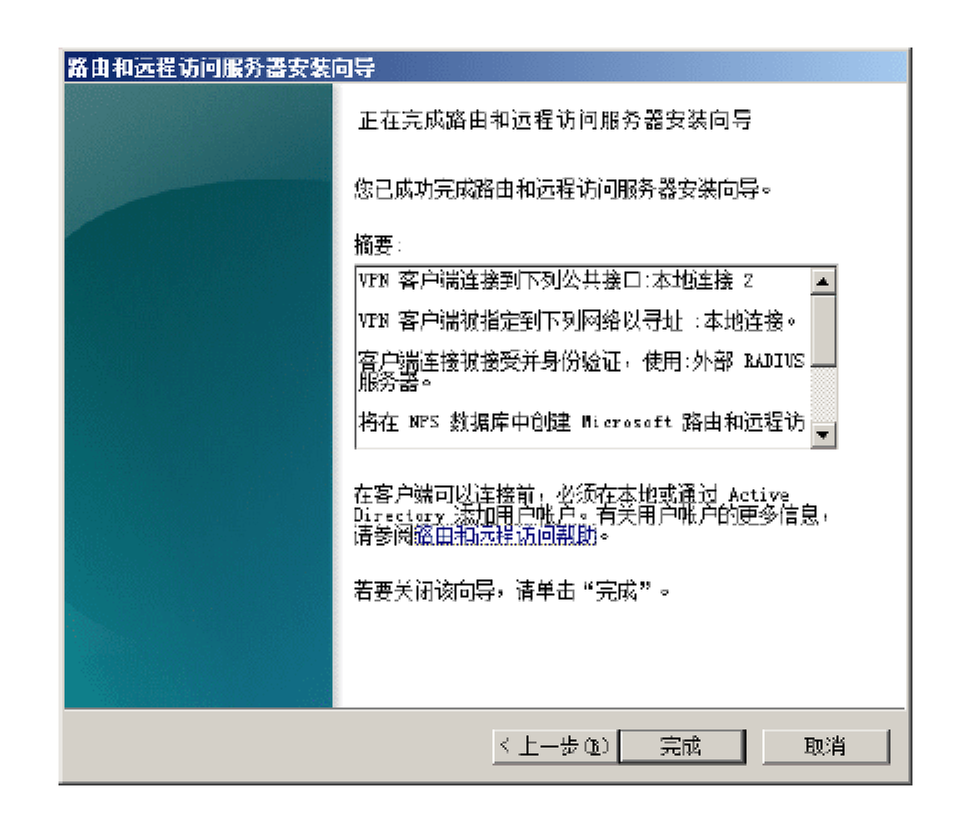


图 11-22 “正在完成路由和远程访问服务器安装向导”界面

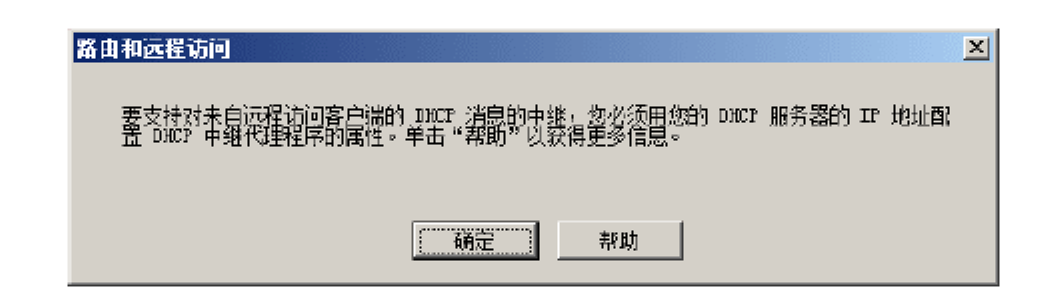


图 11-23 提示框

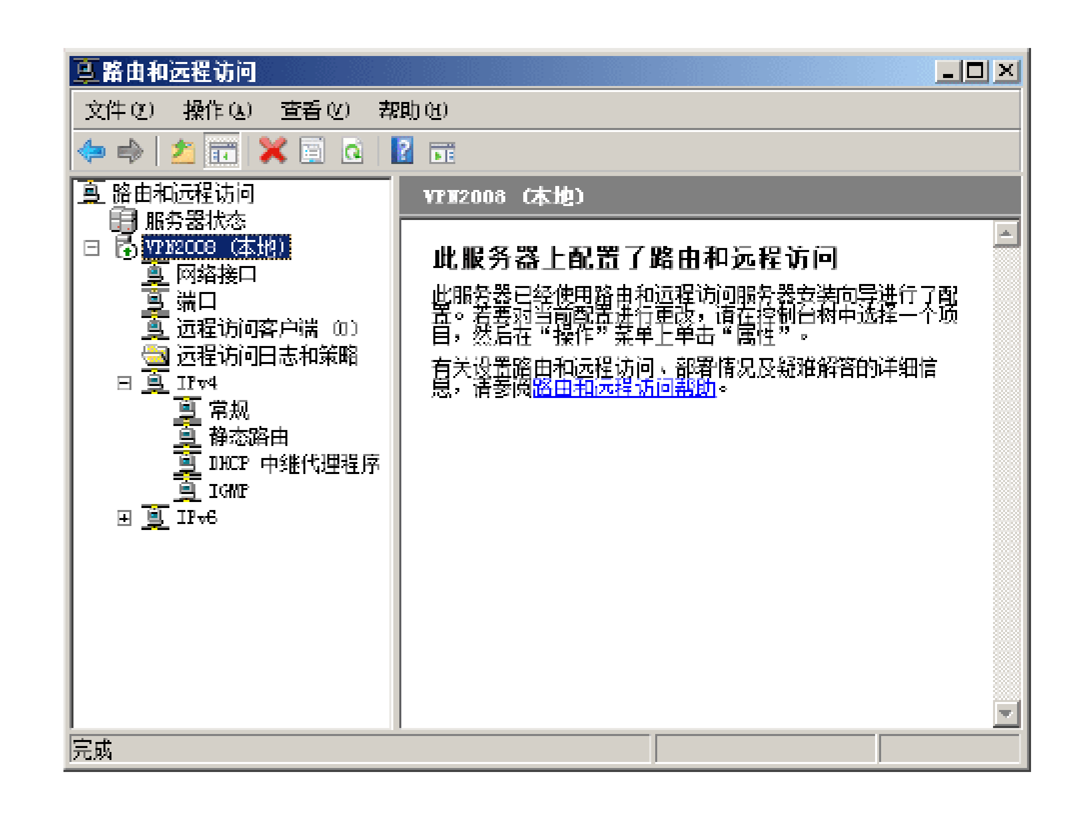


图 11-24 “路由和远程访问”控制台

11.3.5 配置 RADIUS 服务器

在早期版本的 Windows Server 系统中，RADIUS 服务器是基于 IAS 身份验证服务的；在 Windows Server 2008 系统中，该角色是基于 NPS 服务的。建议用户添加 RADIUS 客户端到符合 VPN 服务器的 NPS 服务器中，使用 RADIUS 进行 VPN 连接的身份验证、授权和记账。

1. 配置 RADIUS 身份认证方式

在“路由和远程访问”控制台中，右击 VPN 服务器名，选择快捷菜单中的“属性”命令，打开服务器的属性对话框，切换到“安全”选项卡，确认在“身份验证提供程序”下拉列表框中选择“RADIUS 身份验证”选项，如图 11-25 所示。

单击“身份验证方法”按钮，弹出如图 11-26 所示的“身份验证方法”对话框，确保已选中“可扩展的身份验证协议”和“Microsoft 加密身份验证版本 2”复选框，依次单击“确定”按钮，保存并返回“路由和远程访问”窗口。

2. 在网络策略中授权 VPN 远程访问

默认情况下，VPN 服务器上的 NPS 策略是关闭的，并且禁止任何远程访问。管理员需要在网络策略服

务器上启用该策略，并授予远程访问 VPN 的访问权限。

① 打开“网络策略服务器”窗口，依次展开“策略”→“网络策略”，如图 11-27 所示。

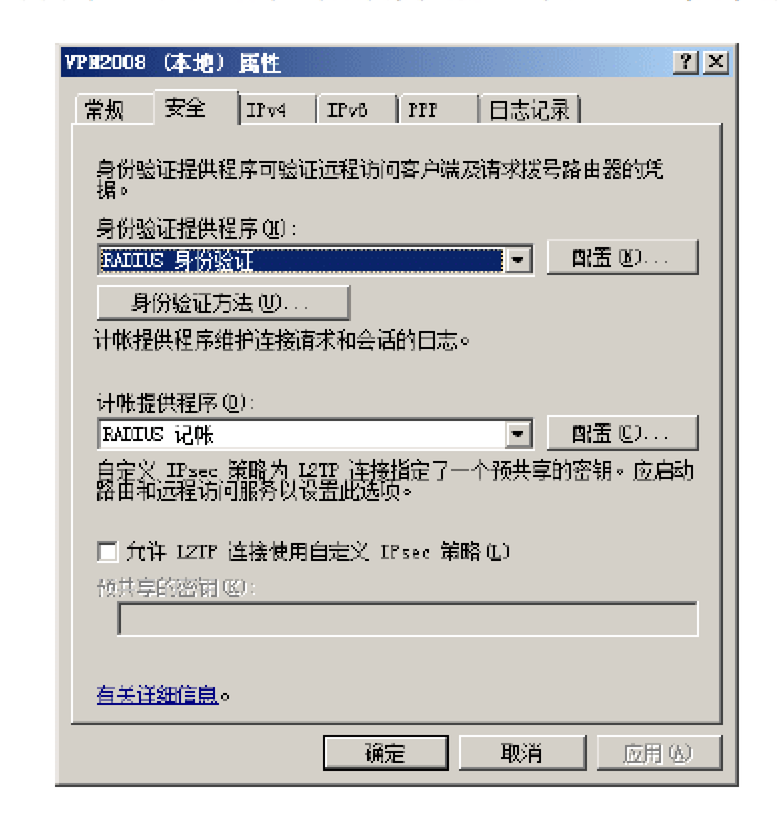


图 11-25　“安全”选项卡

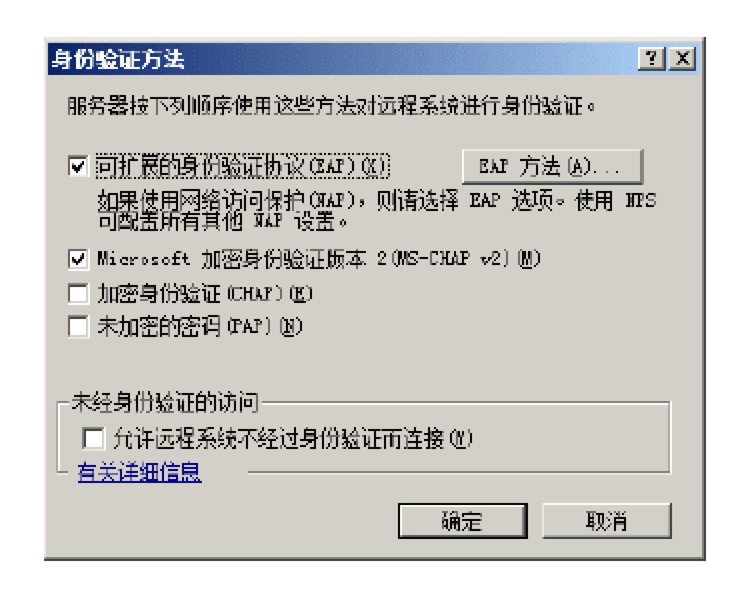


图 11-26　“身份验证方法”对话框

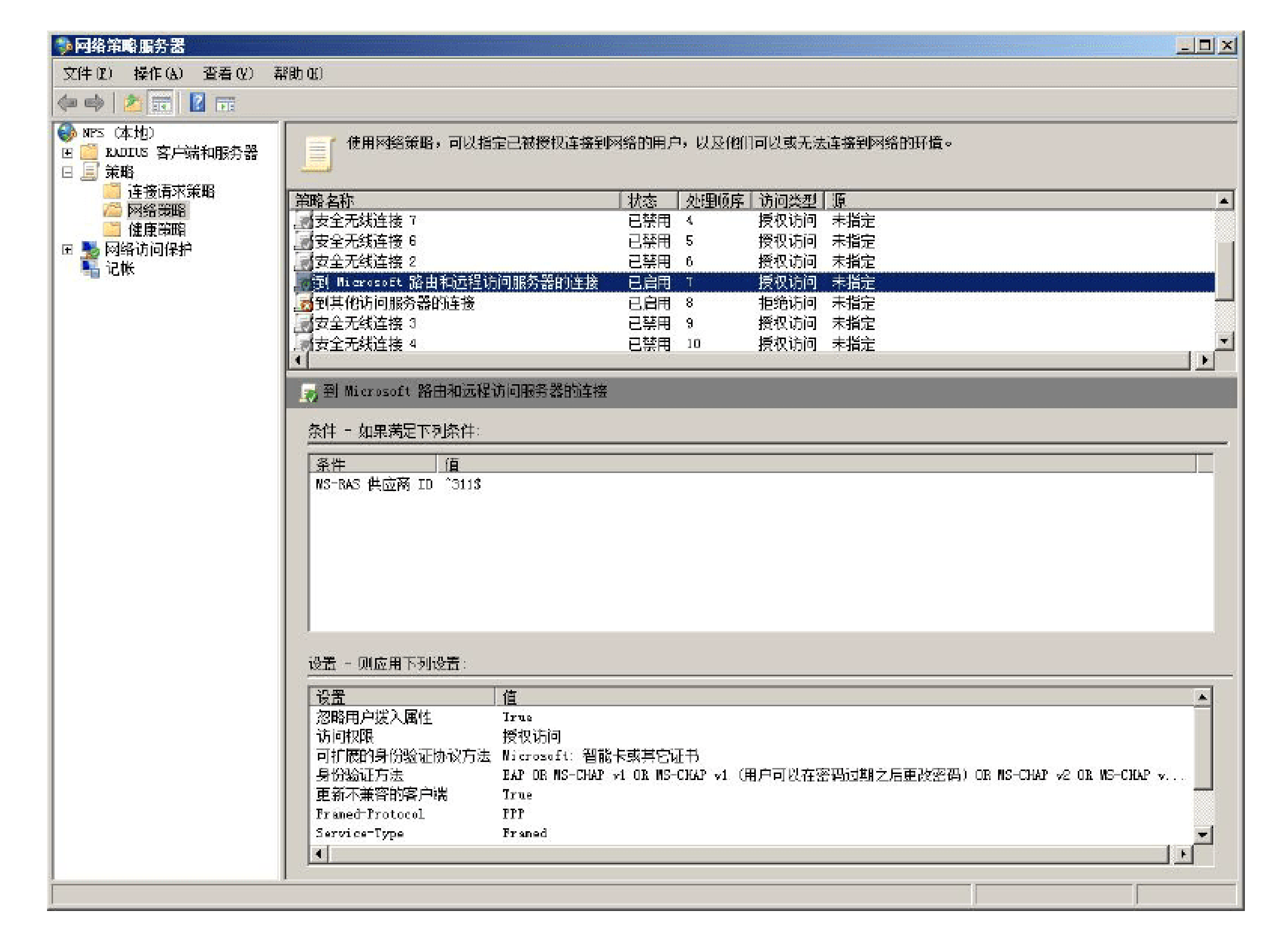


图 11-27　展开“网络策略”

② 双击名为“到 Microsoft 路由和远程访问服务器的连接”的网络策略，显示如图 11-28 所示的“到 Microsoft 路由和远程访问服务器的连接 属性”对话框。在“概述”选项卡中的“访问权限”选项区域中选择“授予访问权限”单选按钮。在“网络连接方法”选项区域的“网络访问服务器的类型”下拉列表框中，选择“远程访问服务器(VPN-Dail up)”选项。

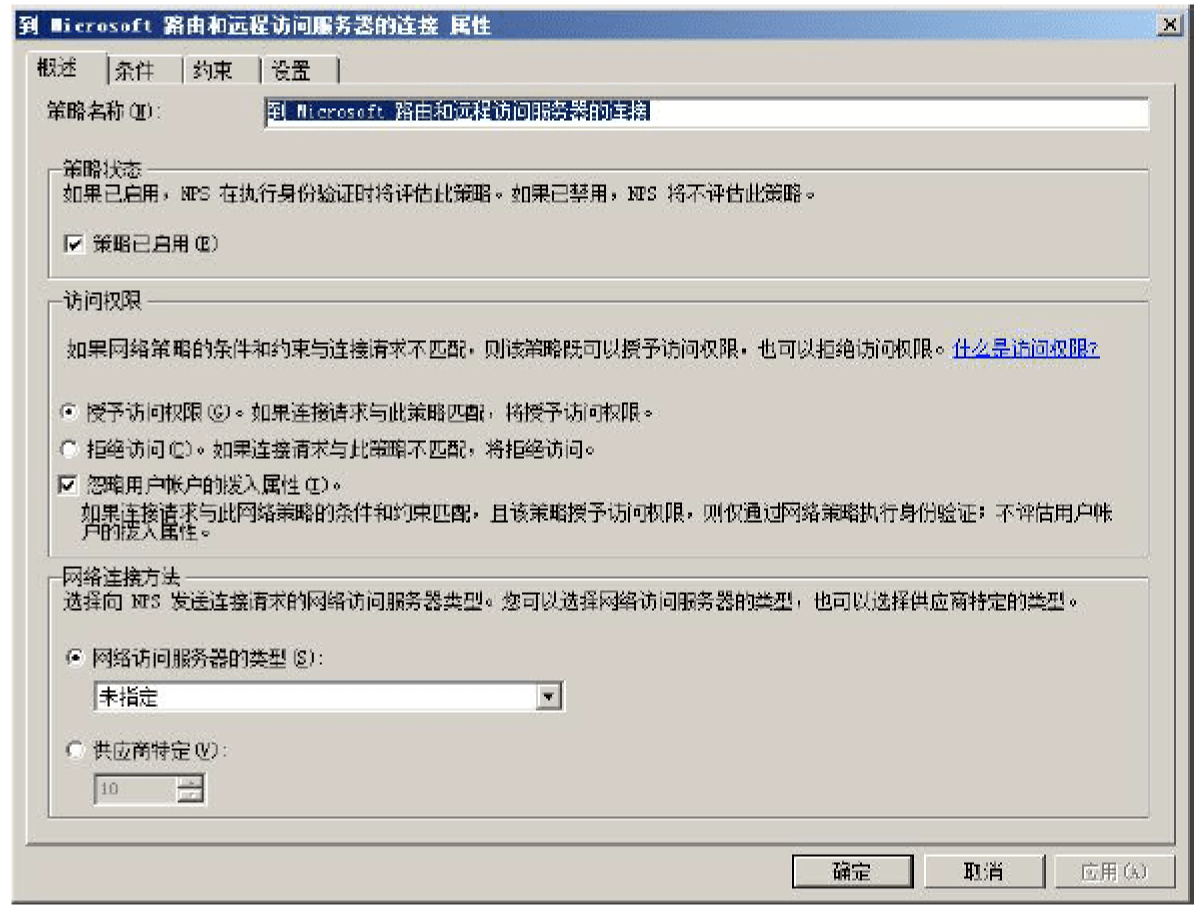
③ 单击“确定”按钮，保存配置。

3. 配置远程访问 VPN 连接策略

连接策略主要用于确保 VPN 客户端系统的健康程度，虽不是 VPN 连接的必要操作，但正确配置之后

可以大大增强 VPN 连接的可靠性和安全性。

① 打开“网络策略服务器”窗口，单击 NPS，显示“入门”页面。在“标准配置”下，从下拉列表框中选择“用于拨号或 VPN 连接的 RADIUS 服务器”选项，单击“配置 VPN”超级链接，显示如图 11-29 所示的“选择拨号或虚拟专用网络连接类型”界面。选择“虚拟专用网络(VPN)连接”单选按钮，输入新 NPS 网络策略的名称。



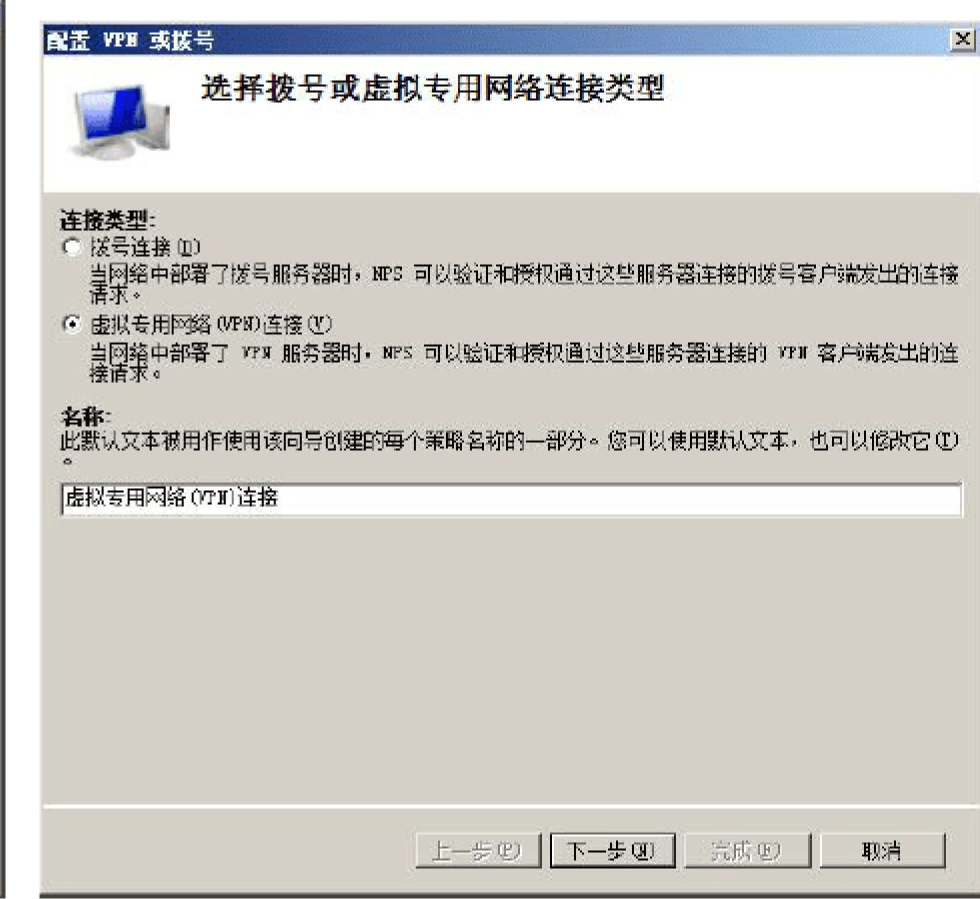


图 11-28 “到 Microsoft 路由和远程访问服务器的连接 属性”对话框

图 11-29 “选择拨号或虚拟专用网络连接类型”界面

② 单击“下一步”按钮，显示如图 11-30 所示的“指定拨号或 VPN 服务器”界面，根据 VPN 服务器的需要添加 RADIUS 客户端。

③ 单击“下一步”按钮，显示如图 11-31 所示的“配置身份验证方法”界面。为了启用和配置 EAP 身份验证类型，选中“可扩展身份验证协议”复选框，在“类型”下拉列表框中选择一个 EAP 类型，然后根据需要单击“配置”按钮，来配置所需要的身份验证方法。





图 11-30 “指定拨号或 VPN 服务器”界面

图 11-31 “配置身份验证方法”界面

④　单击“下一步”按钮，显示如图 11-32 所示的“指定用户组”界面，添加包含允许建立 VPN 远程访问连接的用户账户组。

⑤　单击“下一步”按钮，显示如图 11-33 所示的“指定 IP 筛选器”界面，根据需要添加 IPv4 和 IPv6 输入和输出数据包筛选器，应用于所有远程访问 VPN 连接中。



图 11-32　“指定用户组”界面



图 11-33　“指定 IP 筛选器”界面

⑥　单击“下一步”按钮，显示如图 11-34 所示的“指定加密设置”界面，启用允许的加密强度。

⑦　单击“下一步”按钮，显示如图 11-35 所示的“指定一个领域名称”界面，指定领域的名称，并根据需要选中“进行身份验证前，从用户名中删除领域名称”复选框。

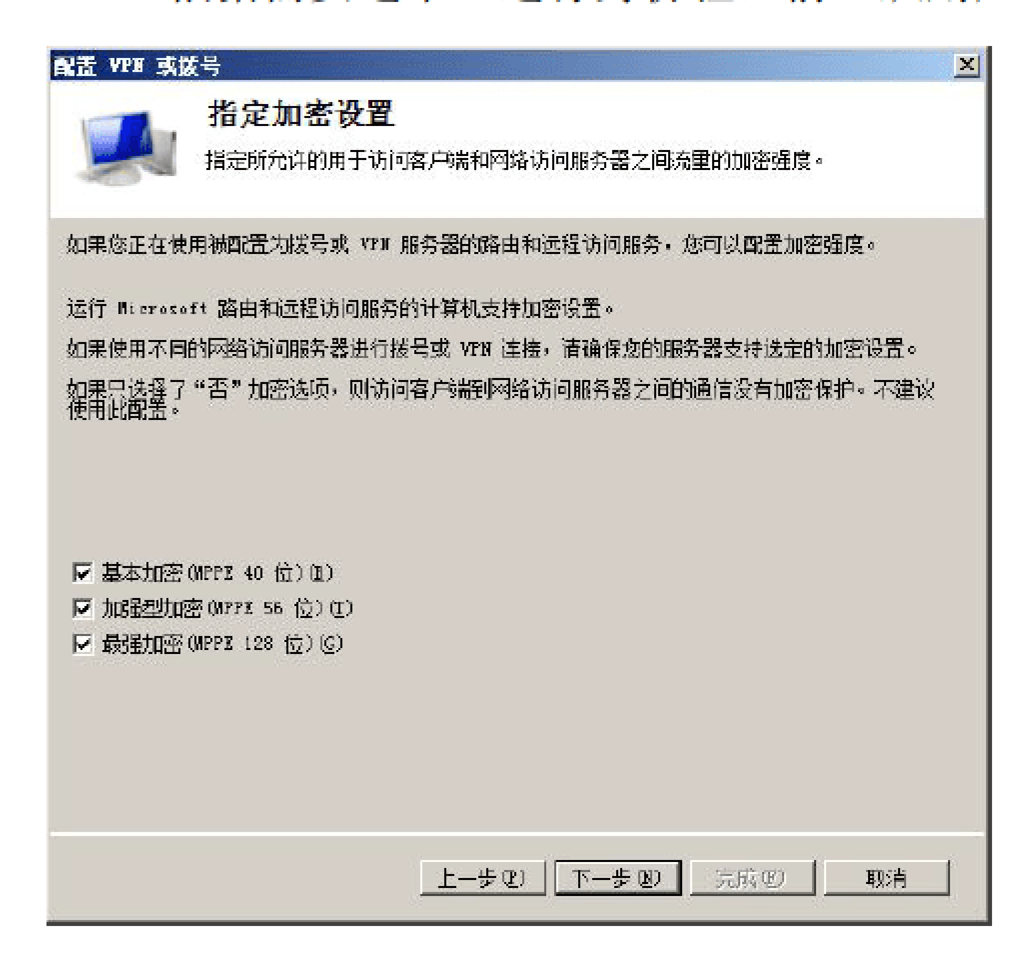






图 11-34　“指定加密设置”界面

图 11-35　“指定一个领域名称”界面

⑧　单击“下一步”按钮，显示如图 11-36 所示的“完成新建拨号或虚拟专用网络连接和 RADIUS 客户端”界面，单击“完成”按钮。

“配置 VPN 或拨号”向导为远程访问 VPN 连接创建了一个连接请求策略和一个网络策略。“配置 VPN 或拨号”向导使用单一 EAP 方式配置网络策略。对于其他 EAP 方式，用户可以从网络策略属性中的“设置”选项卡中配置。在用户使用适当的日志、RADIUS 客户端和策略设置配置完主 NPS 服务器后，复制配置到

辅助或其他 NPS 服务器上。



图 11-36 “完成新建拨号或虚拟专用网络连接和 RADIUS 客户端”界面

11.3.6 配置内网基础结构

VPN 远程连接的最终目的是以最安全的方式访问内网资源，因此仅建立 VPN 客户端到 VPN 服务器的连接是不够的。管理员必须为远程拨入用户设置路由信息，以确保其可以访问内网服务器或网络设备。为了使 VPN 服务器能够在内网中正确转发通信，用户必须完成如下工作之一。

- 添加概括内网中所使用的 IPv4 和 IPv6 地址空间的静态路由。
- 如果用户在内网子网中使用 RIP IPv4 路由连接 VPN 服务器，那么添加 RIP 路由协议，保证 VPN 服务器可以与临近的 RIP 路由器交换路由，并且为内网子网自动添加路由到路由表中。

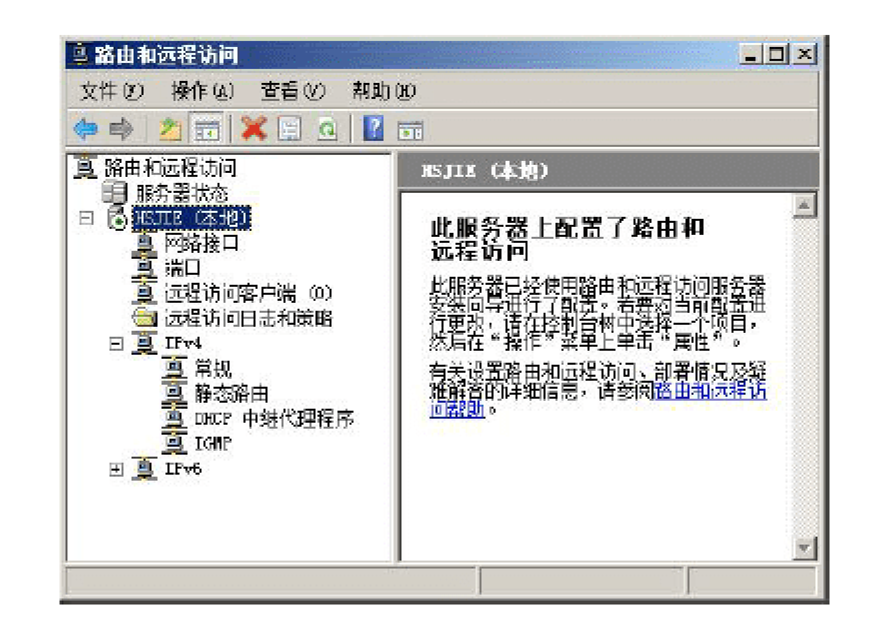


图 11-37 “路由和远程访问”窗口

1. 添加 IPv4 静态路由

① 打开“路由和远程访问”窗口，在左侧的控制台中展开 IPv4 节点，如图 11-37 所示。

② 右击“静态路由”，在弹出的快捷菜单中选择“新建静态路由”命令，显示如图 11-38 所示的“IPv4 静态路由”对话框，为静态路由选择适当的接口，然后输入目标、网络掩码、网关和跃点数。



提示：重复此操作可以添加到其他子网的 IPv4 静态路由。

③ 单击“确定”按钮保存设置。

IPv6 静态路由的创建与 IPv4 完全相同，此处不复赘述。

2. 配置 VPN 服务器作为 RIP 路由器

① 打开“路由和远程访问”窗口，在左侧的控制台中展开 IPv4 节点。右击“常规”，在弹出的快捷菜单中选择“新建路由协议”命令，显示如图 11-39 所示的“新路由协议”对话框，选择“用于 Internet 协议的 RIP 版本 2”路由协议。



图 11-38　“IPv4 静态路由”对话框



图 11-39　“新路由协议”对话框

② 单击“确定”按钮返回“路由和远程访问”窗口。

③ 右击 RIP，在弹出的快捷菜单中选择“新增接口”命令，显示如图 11-40 所示的“用于 Internet 协议的 RIP 版本 2 的新接口”对话框，选择 VPN 服务器的内网接口即可。

④ 单击“确定”按钮，显示如图 11-41 所示的“RIP 属性”对话框，根据 VPN 服务器的内网子网中临近 RIP 路由器配置 RIP 路由协议。



图 11-40　“用于 Internet 协议的 RIP 版本 2 的新接口”对话框

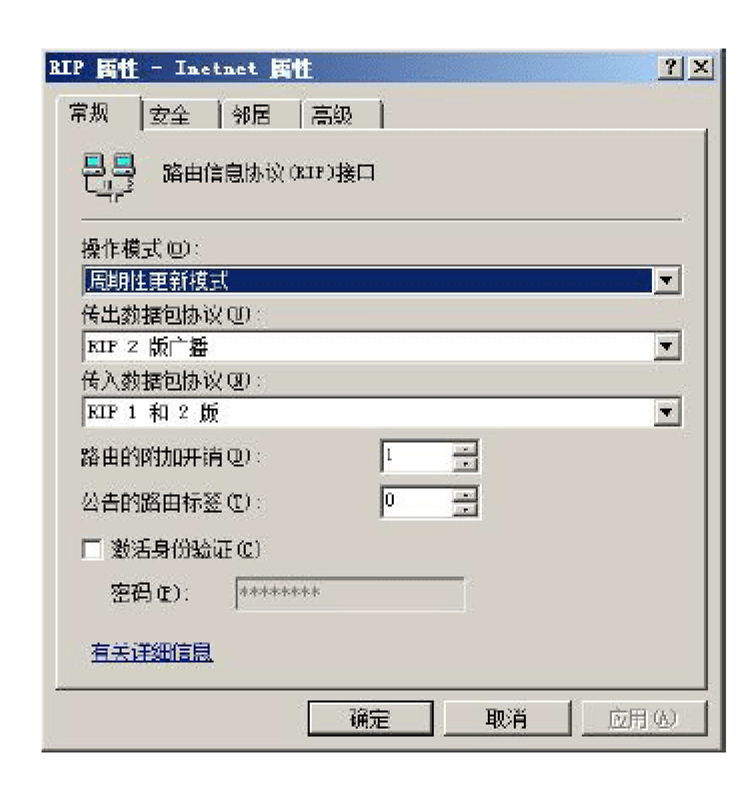


图 11-41　“RIP 属性”对话框

⑤ 单击“确定”按钮，保存配置。

11.3.7　配置 VPN 客户端

配置 VPN 客户端的关键之处在于，客户端必须选择与服务器端匹配的身份验证方式和加密协议。通常情况下，管理员可以通过手动和 CM 配置文件两种方式配置 VPN 客户端。客户端创建 VPN 连接之后，默认将自动断开到其他 Internet 主机的连接。因此，若想同时访问 VPN 连接与 Internet，则可以手动创建 VPN 所需的静态路由，避免其自动创建。

1. 手动配置 VPN 客户端

如果用户拥有少量的 VPN 客户端，用户可以为每台 VPN 客户端手动配置 VPN 连接。对于 Windows Server 2008 和 Windows Vista VPN 客户端，使用“设置连接或网络”向导；对于 Windows XP 和 Windows Server 2003 VPN 客户端，使用“新建连接向导”。

(1) 创建 VPN 客户端连接

① 登录到 Windows Vista 系统以后，首先使用 ADSL 或其他接入方式连接到 Internet。

② 打开“网络和共享中心”窗口，单击“设置连接或网络”链接，显示“选择一个连接选项”界面，选择“连接到工作区”选项，如图 11-42 所示。

③ 单击“下一步”按钮，显示如图 11-43 所示的“您想如何连接”界面，选择建立 VPN 连接的方式。

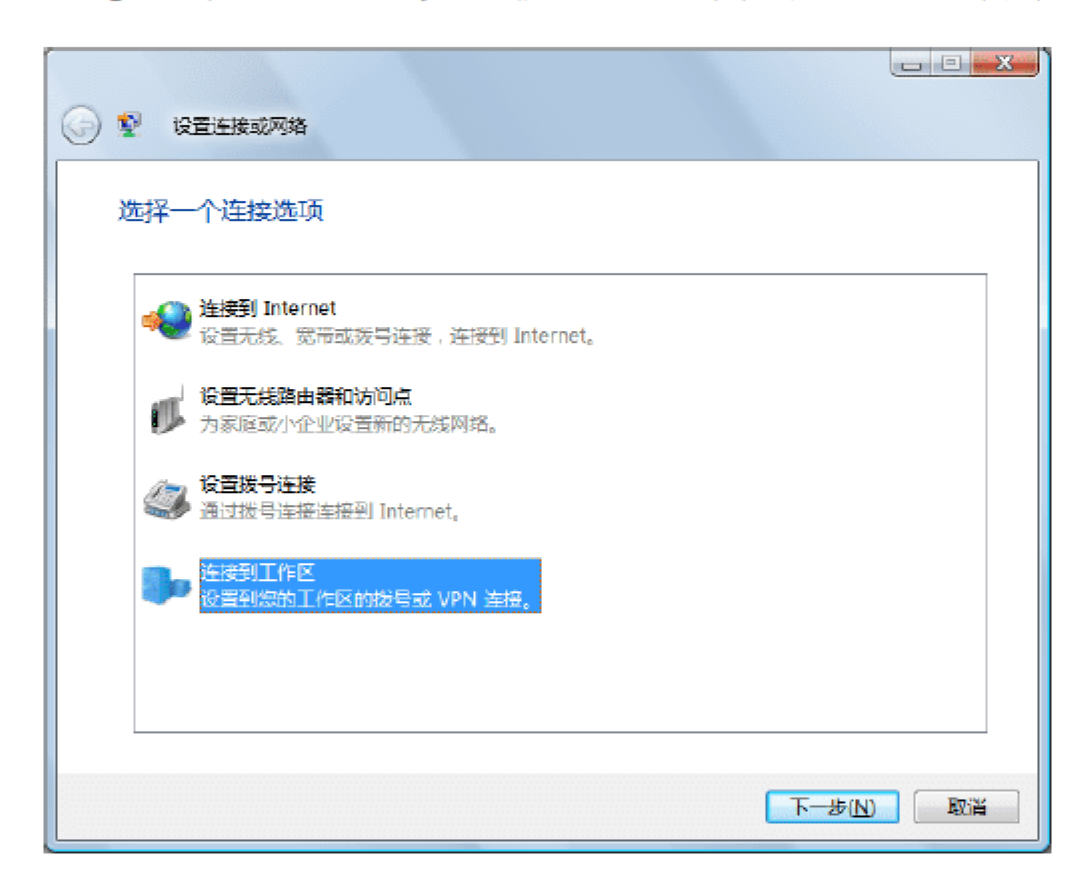


图 11-42 “选择一个连接选项”界面



图 11-43 “您想如何连接”界面

④ 单击“使用我的 Internet 连接(VPN)”选项，显示如图 11-44 所示的“键入要连接的 Internet 地址”界面，在“Internet 地址”文本框中输入 VPN 服务器的域名或公网 IP 地址。可以是 IPv4 地址，也可以是 IPv6 地址。在“目标名称”文本框中输入进行 VPN 连接时显示的名称。



提示：智能卡是包含用户账户重要信息的芯片，使用时将个人专用智能卡插入计算机的读卡器即可。使用智能卡可以提供比密码更高的安全级别，当然成本也较高。

⑤ 单击“下一步”按钮，显示如图 11-45 所示的“键入您的用户名和密码”界面。分别在“用户名”和“密码”文本框中，输入用于 VPN 拨入的用户账户和密码，为了便于下次使用，可选中“记住此密码”复选框。在“域”文本框中输入域名。

⑥ 单击“连接”按钮，开始尝试连接到远程 VPN 服务器，如图 11-46 所示。

⑦ 不过，此时并不能连接到 VPN 服务器，会显示如图 11-47 所示的“向导无法连接”界面。单击“仍然设置连接”按钮，保存该 VPN 连接。

注意：如果网络中没有配置 NPS 服务器，而仅仅使用 VPN 拨入功能，则在为用户赋予拨入权限时，必须选择“允许访问”选项，否则无法拨入内部网络。当使用 VPN 连接到内部网络以后，就如同在局域网中一样，在浏览网页、运行各种应用程序时都是通过 VPN 网络的 Internet 连接接入的。

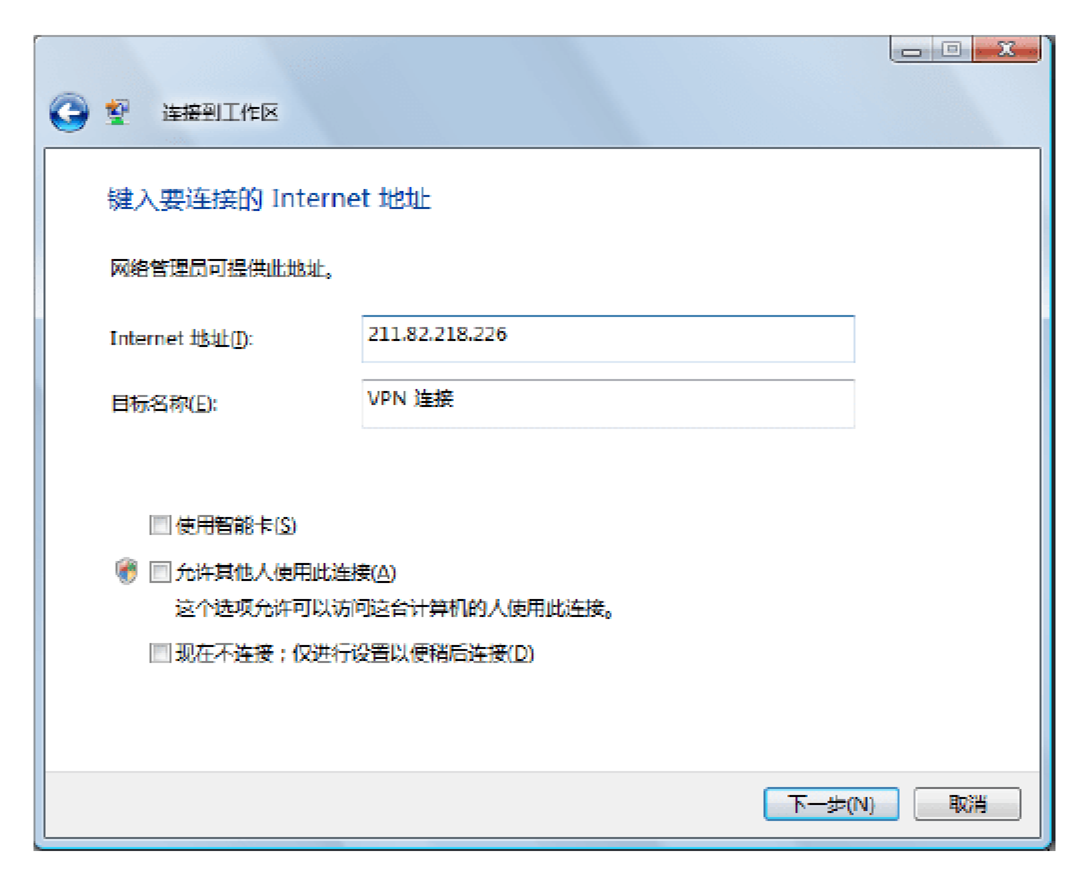


图 11-44　“键入要连接的 Internet 地址”界面

图 11-45　“键入您的用户名和密码”界面

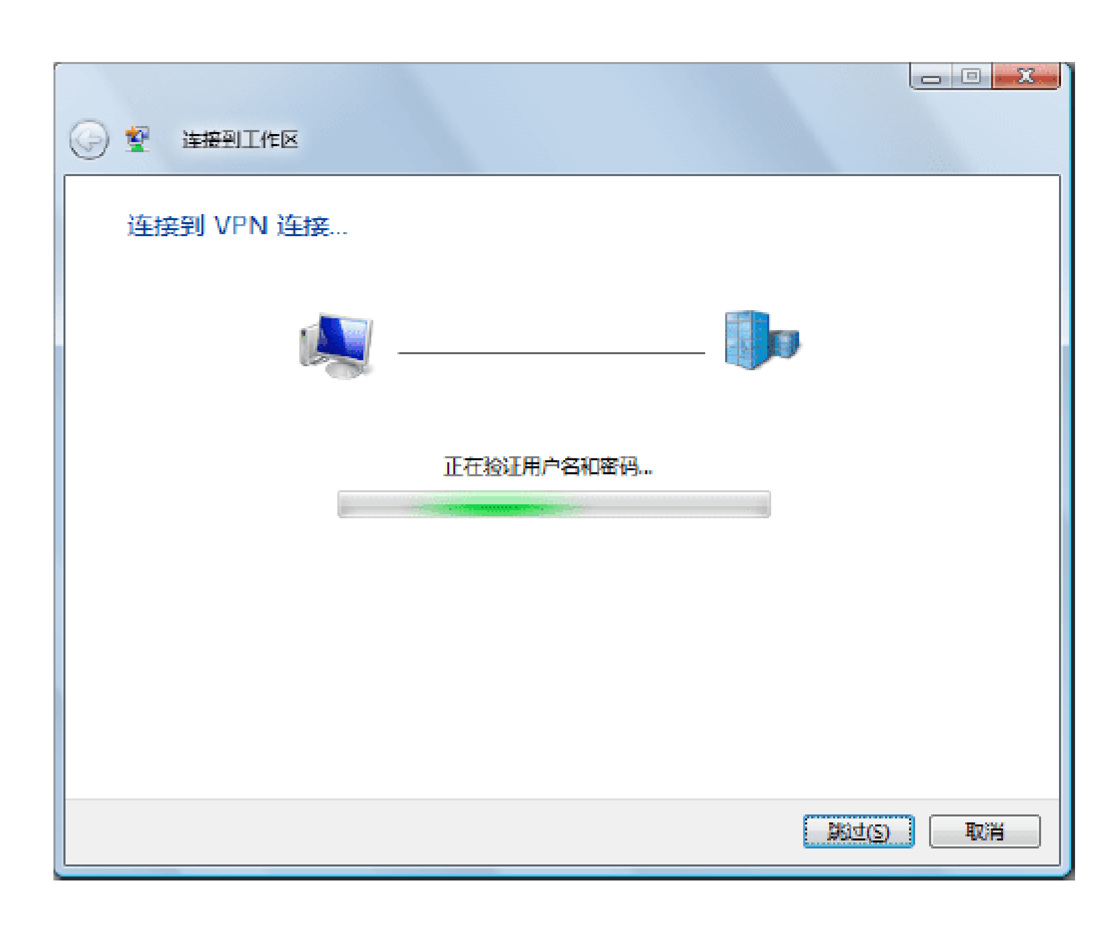


图 11-46　尝试连接到远程 VPN 服务器

图 11-47　“向导无法连接”界面

(2) 配置身份验证协议

① 在“网络和共享中心”窗口中，单击“管理网络连接”打开“网络连接”窗口。选择已创建的 VPN 链接，右击并选择快捷菜单中的“属性”选项，显示如图 11-48 所示的“VPN 连接 属性”对话框。

② 切换到“安全”选项卡，选择“高级(自定义设置)”单选按钮，如图 11-49 所示。

③ 单击“设置”按钮，显示如图 11-50 所示的“高级安全设置”对话框，在“数据加密”下拉列表框中选择“需要加密(如果服务器拒绝将断开连接)”选项。选择“使用可扩展的身份验证协议(EAP)”单选按钮，并在其下拉列表框中选择“受保护的 EAP (PEAP) (启用加密)”选项。

④ 单击“属性”按钮，显示如图 11-51 所示的“受保护的 EAP 属性”对话框，确认选中“验证服务器证书”复选框，并取消选中“连接到这些服务器”复选框。在“受信任的根证书颁发机构”列表框中，可以看到已经安装的证书颁发机构。在“选择身份验证方法”下拉列表框中，选择“安全密码”选项，并选中“启用隔离检查”复选框。

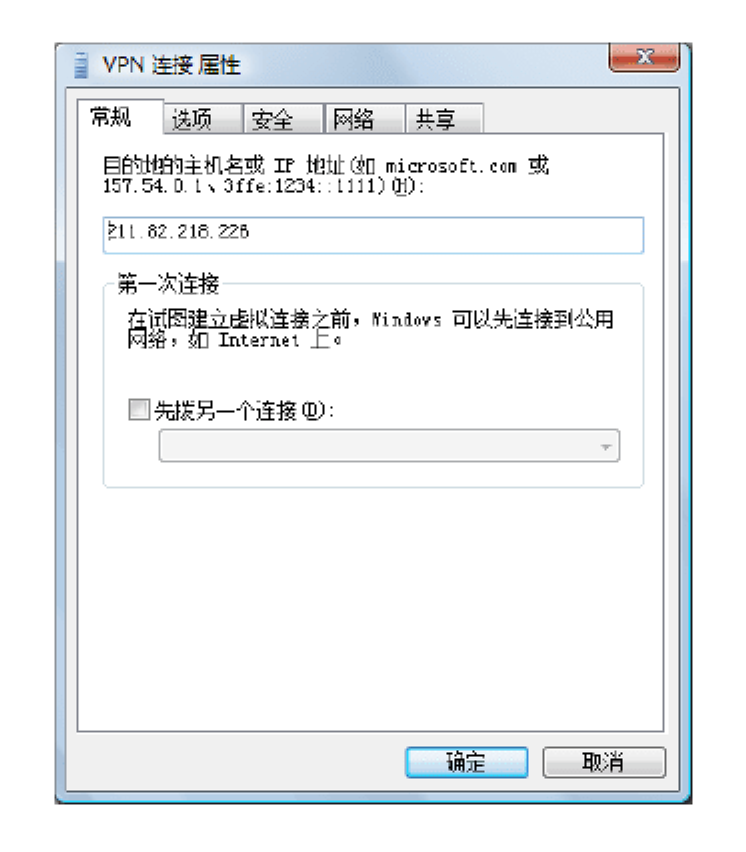


图 11-48 “VPN 连接 属性”对话框

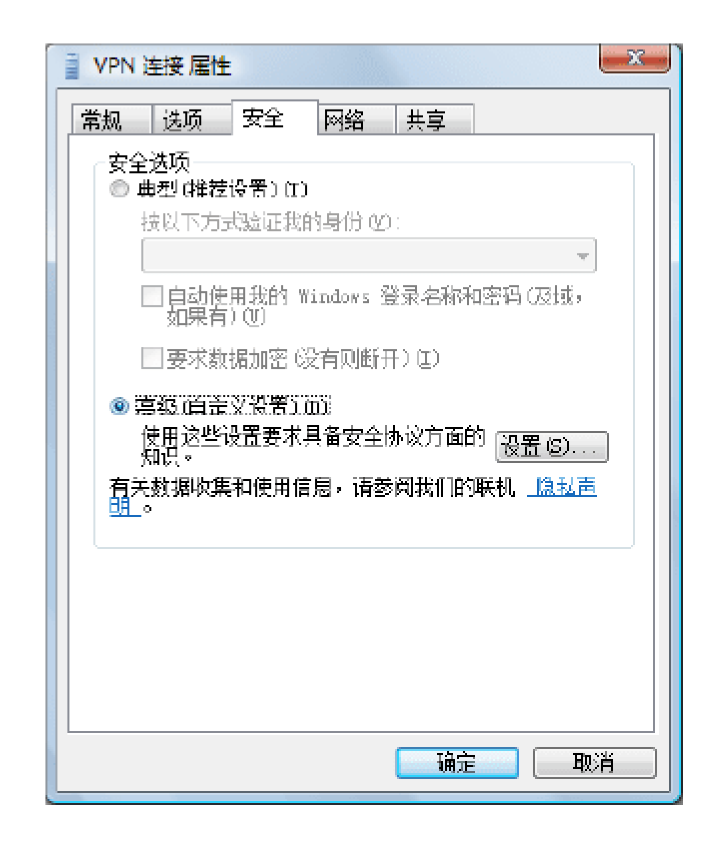


图 11-49 “安全”选项卡

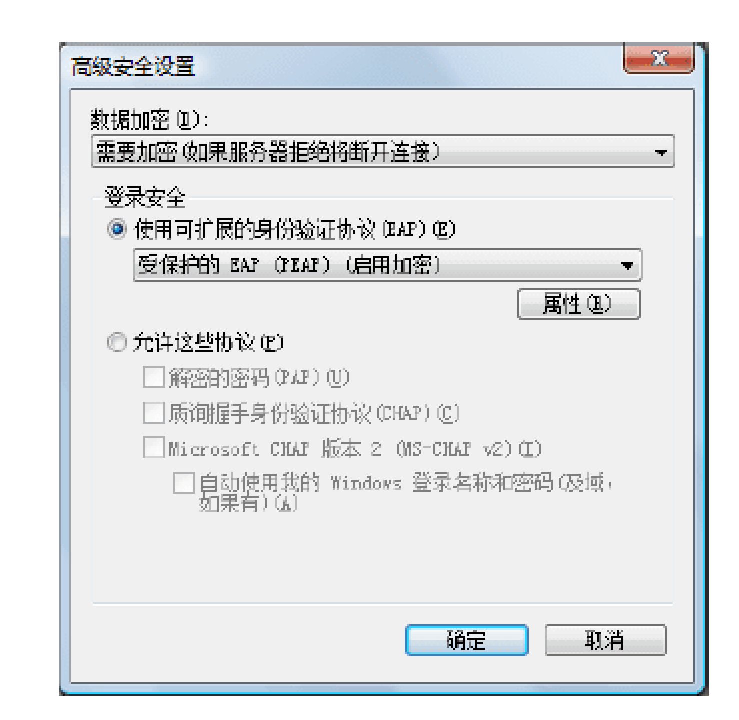


图 11-50 “高级安全设置”对话框

⑤ 依次单击“确定”按钮保存配置即可。

2. 使用 CM 配置文件部署客户端

对于大量的运行不同版本 Windows 系统的 VPN 客户端，管理员可以使用 CMAK 为用户创建 CM 配置文件。完成之后，通过相应的方式发送到客户端即可。创建 VPN 连接客户端的用户只需执行 CM 配置文件，系统即可自动创建 VPN 连接。

(1) 安装 CMAK 功能组件

默认情况下，Windows Server 2008 系统并未安装 CMAK 功能组件，管理员可以通过“服务器管理器”中的“添加功能”来安装“连接管理器管理工具包”。

① 依次单击“开始”→“管理工具”→“服务器管理器”命令，显示“服务器管理器”对话框。单击“功能”，在详细面板中单击“添加功能”超级链接，显示如图 11-52 所示的“选择功能”界面，选中“连接管理器管理工具包”复选框。

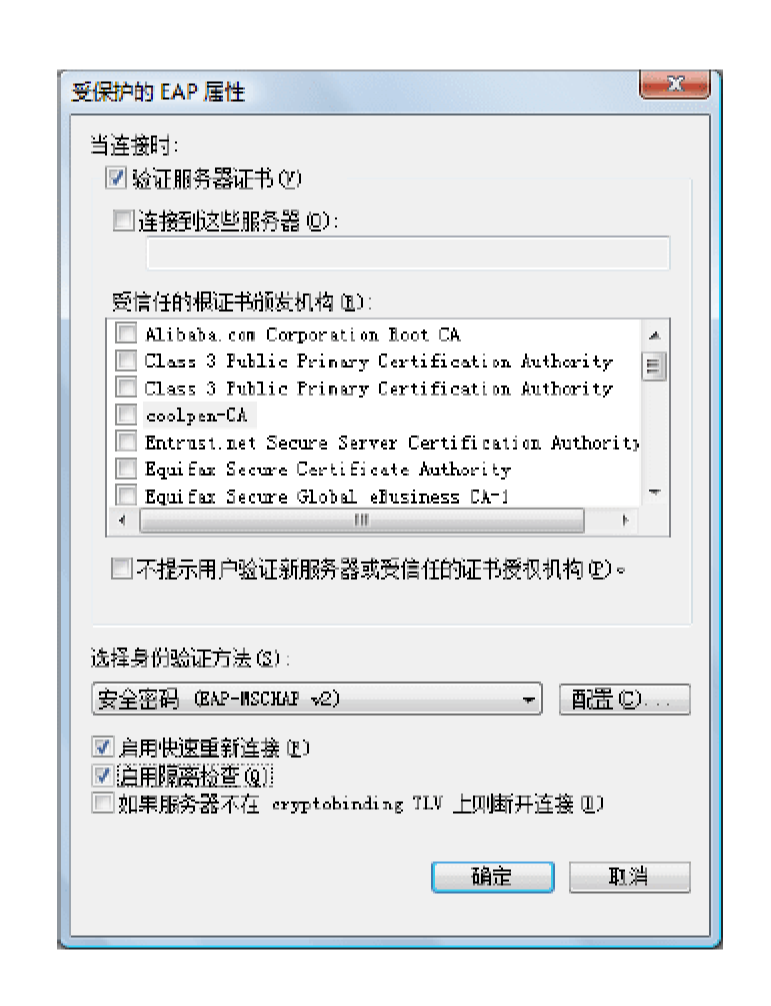


图 11-51 “受保护的 EAP 属性”对话框



图 11-52 “选择功能”界面

② 单击“下一步”按钮，显示如图 11-53 所示的“确认安装选择”界面。单击“安装”按钮，显示“安装进度”界面，从中可以看出安装进度情况。

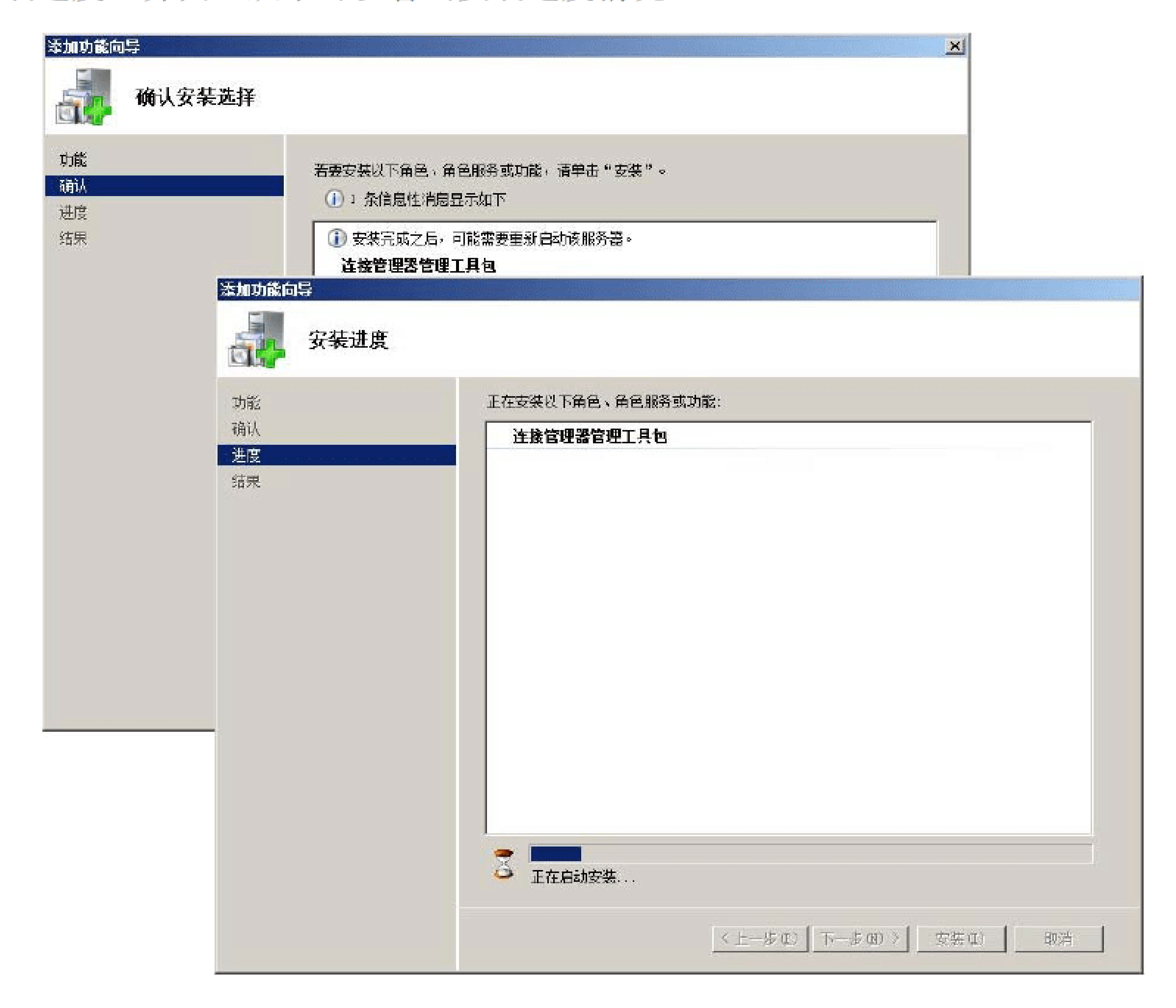


图 11-53　“确认安装选择”界面

③ 安装完成后，显示如图 11-54 所示的“安装结果”界面。单击“关闭”按钮即可。



图 11-54　“安装结果”界面

(2) 为 VPN 连接创建 CM 配置文件

① 依次单击“开始”→“管理工具”→“连接管理器管理工具包”命令，显示如图 11-55 所示的“欢迎使用‘连接管理器管理工具包向导’”界面。

② 单击“下一步”按钮，显示如图 11-56 所示的“选择目标操作系统”界面，根据分配 CM 配置文件的 VPN 客户端的设置，选择 Windows Vista 或者“Windows Server 2003、Windows XP 或 Windows 2000”单选按钮。

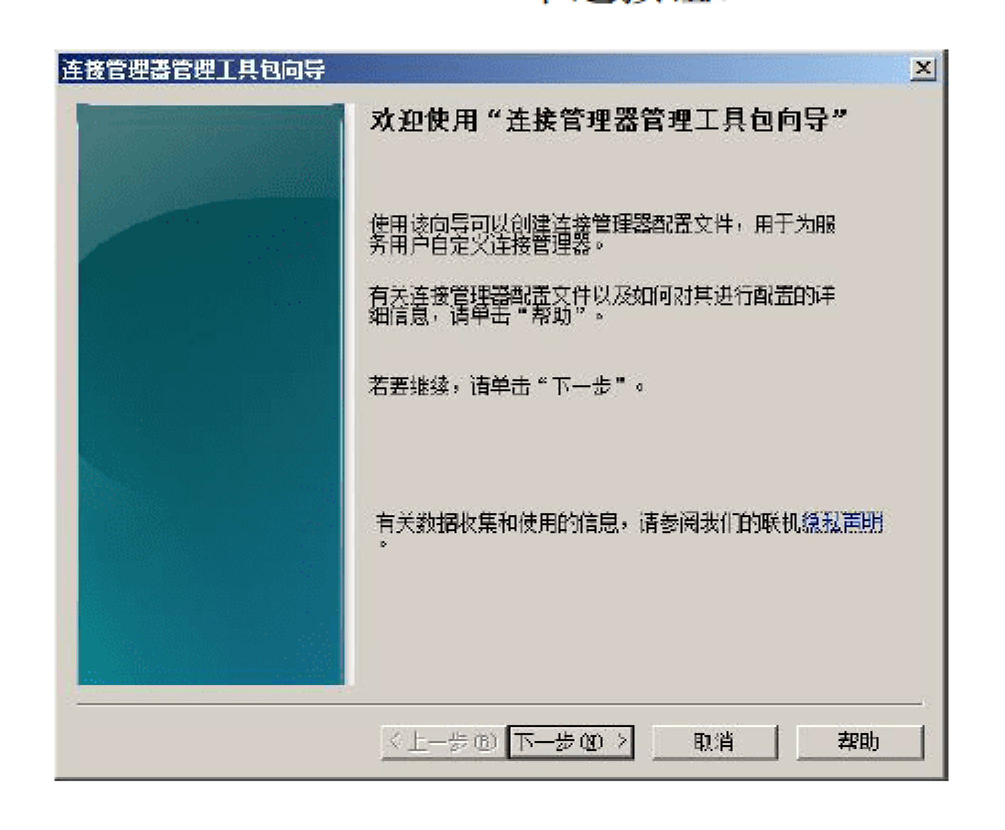


图 11-55 “欢迎使用‘连接管理器管理工具包向导’”界面

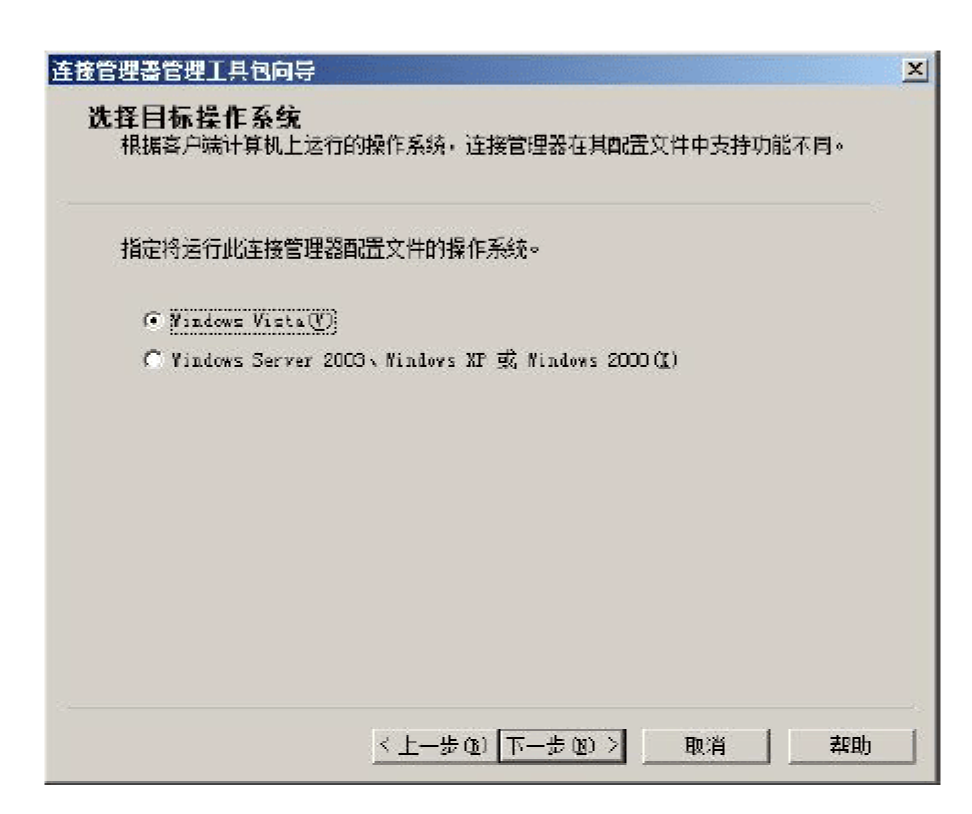


图 11-56 “选择目标操作系统”界面

③ 单击“下一步”按钮，显示如图 11-57 所示的“创建或修改连接管理器配置文件”界面，选择“新建配置文件”单选按钮。

④ 单击“下一步”按钮，显示如图 11-58 所示的“指定服务名称和文件名”界面，输入配置文件创建的网络连接名称和存储在硬盘中的名称。

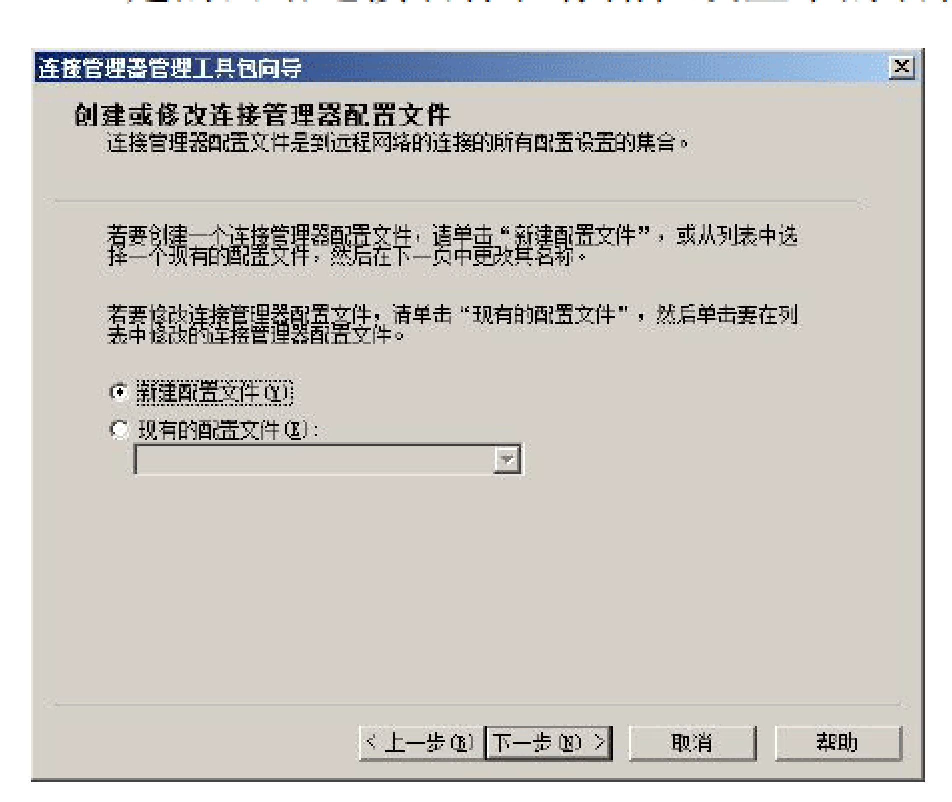


图 11-57 “创建或修改连接管理器配置文件”对话框

图 11-58 “指定服务名称和文件名”对话框

⑤ 单击“下一步”按钮，显示如图 11-59 所示的“指定一个领域名称”界面，配置领域名称，如果不需要指定领域名称，则保持默认设置即可。

⑥ 单击“下一步”按钮，显示如图 11-60 所示的“合并来自其他配置文件的信息”界面，指定需要合并的现有配置文件。

⑦ 单击“下一步”按钮，显示如图 11-61 所示的“添加 VPN 连接的支持”界面，选中“此配置文件的电话簿”复选框。在“VPN 服务器名或 IP 地址”选项区域中输入 VPN 服务器 Internet 接口的 FQDN、公有 IPv4 地址，或者全局 IPv6 地址。

⑧ 单击“下一步”按钮，显示如图 11-62 所示的“创建或修改 VPN 项目”界面。

⑨ 单击“编辑”按钮，显示如图 11-63 所示的“编辑 VPN 项目”对话框，在“常规”、IPv4、IPv6、

“安全”和“高级”选项卡中指定适当的设置。



图 11-59　“指定一个领域名称”界面

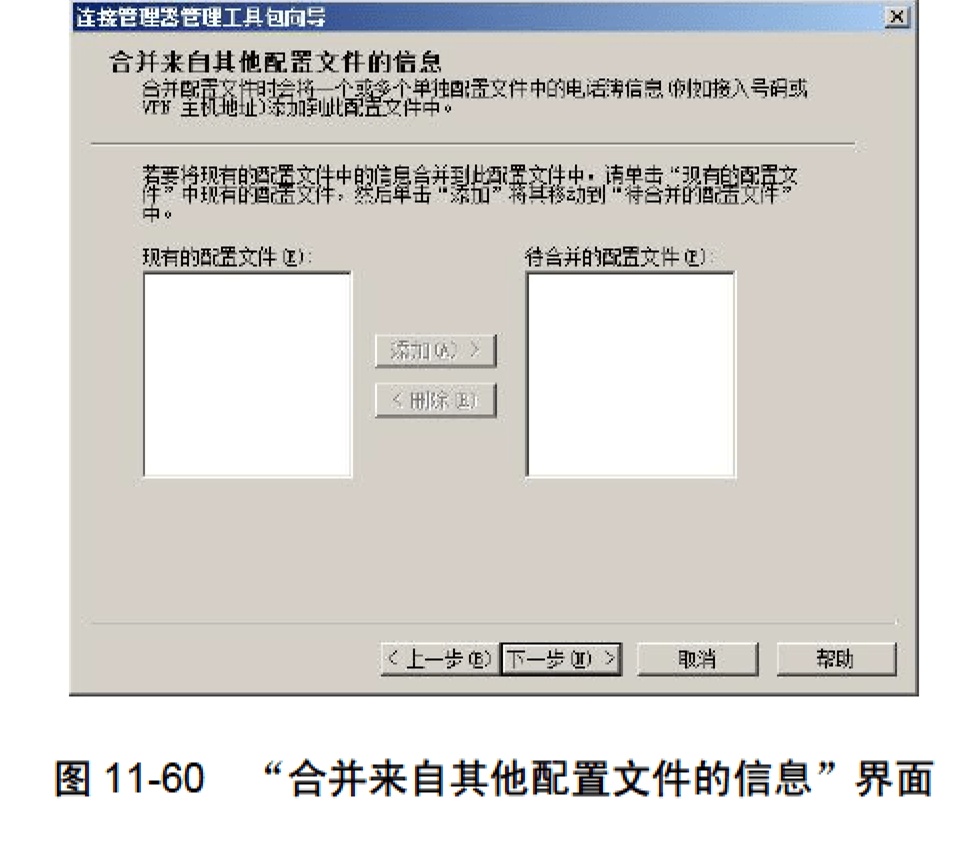


图 11-60　“合并来自其他配置文件的信息”界面



图 11-61　“添加 VPN 连接的支持”界面

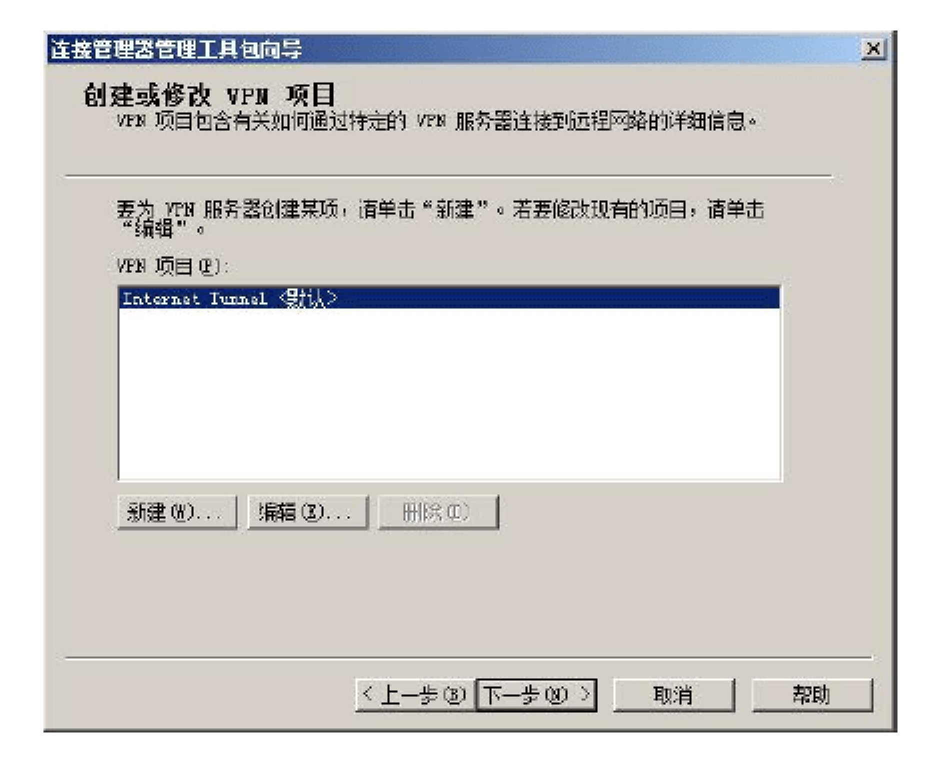


图 11-62　“创建或修改 VPN 项目”界面

⑩　切换至如图 11-64 所示的“安全”选项卡，可以设置“数据加密”、“身份验证方法”和“VPN 战略”。

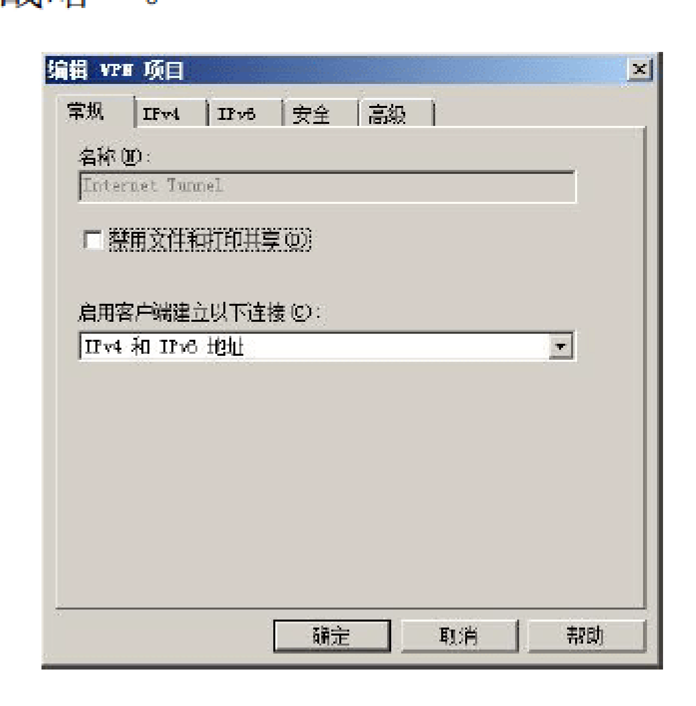


图 11-63　“编辑 VPN 项目”对话框

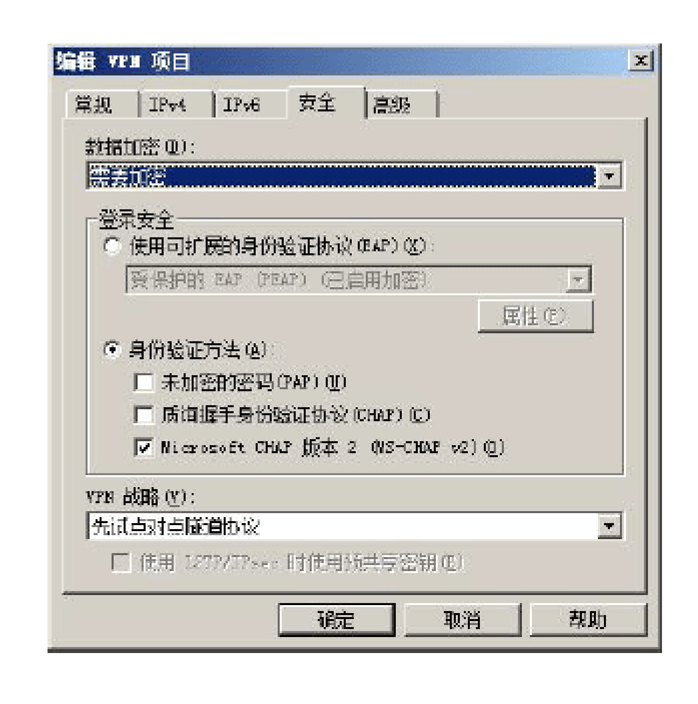


图 11-64　“安全”选项卡

⑪　单击“确定”按钮，返回“创建或修改 VPN 项目”对话框。单击“下一步”按钮，显示如图 11-65 所示的“添加一个自定义电话簿”界面，取消选中“自动下载电话簿更新”复选框。

⑫　单击“下一步”按钮，显示如图 11-66 所示的“配置拨号网络项”界面。

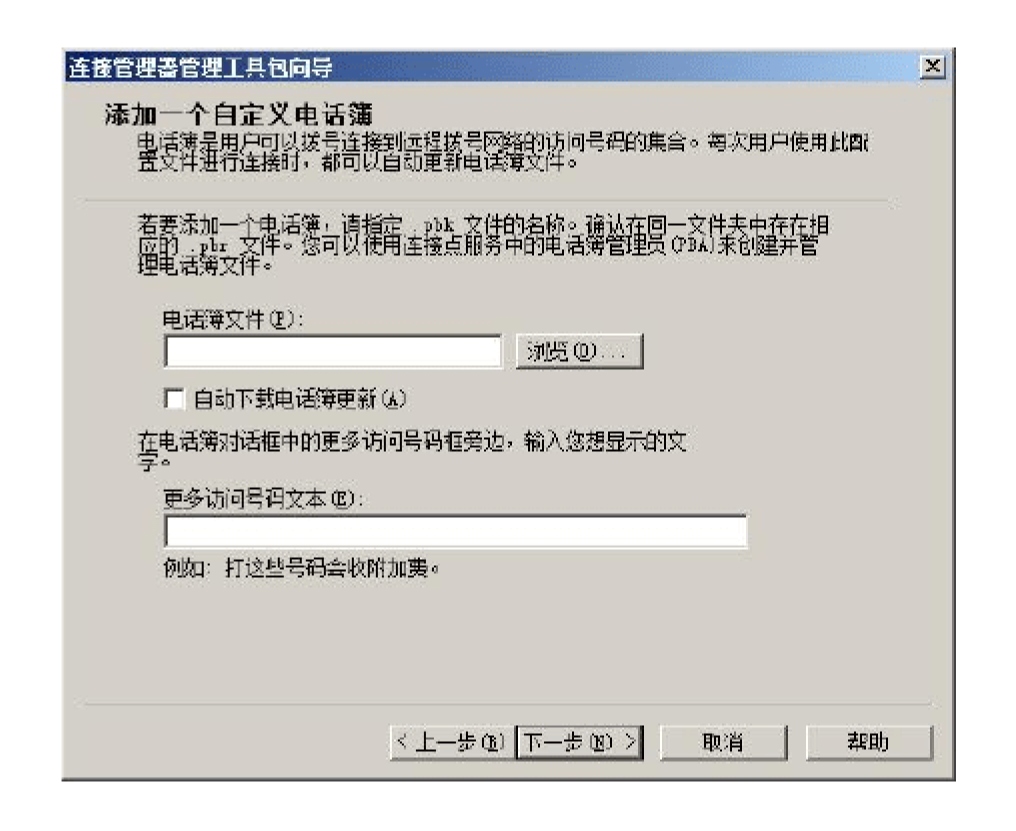


图 11-65 “添加一个自定义电话簿”界面

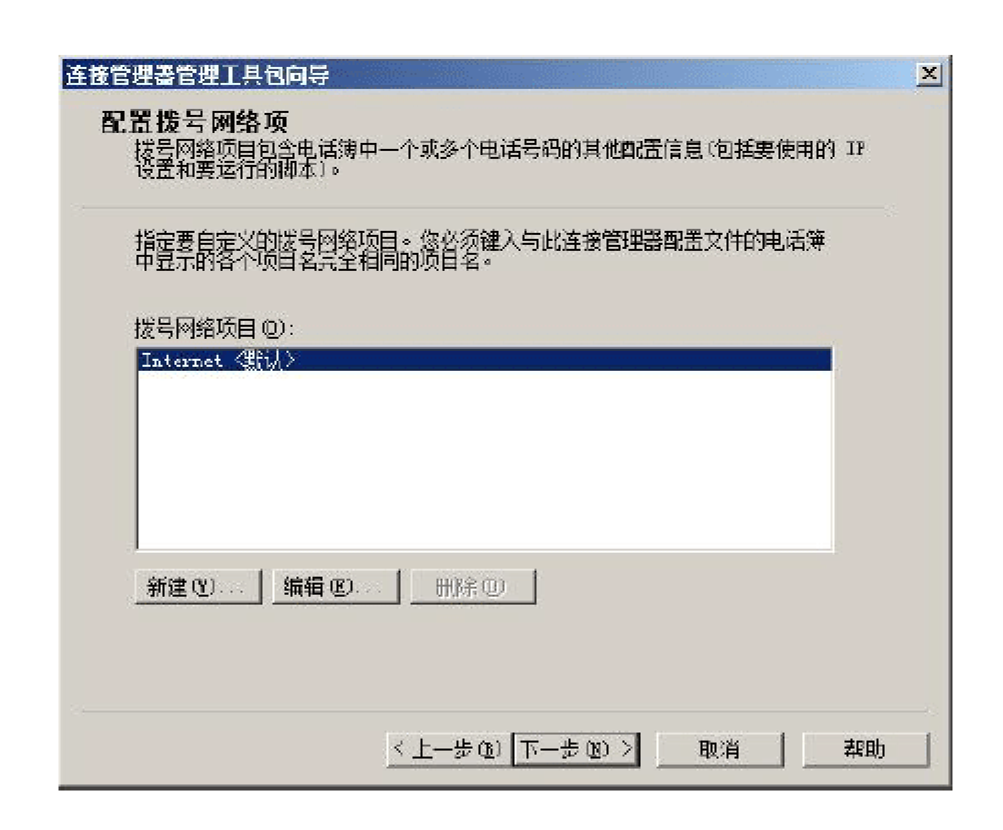


图 11-66 “配置拨号网络项”界面

⑬ 单击“下一步”按钮，显示如图 11-67 所示的“指定路由表更新”界面，如果用户正在使用 CM 配置文件为 VPN 服务器的并发 Internet 访问和内网访问添加路由，则选择“定义路由表更新”单选按钮，并指定包含路由或 URL 的文件。

⑭ 单击“下一步”按钮，显示如图 11-68 所示的“配置 Internet Explorer 的代理设置”界面，如果用户想要在内网中使用代理服务器配置 VPN 客户端，选择“自动将当前用户的 Internet Explorer 代理设置复制到隧道接口”或者“自动配置代理设置”单选按钮，然后指定包含代理设置的文件。

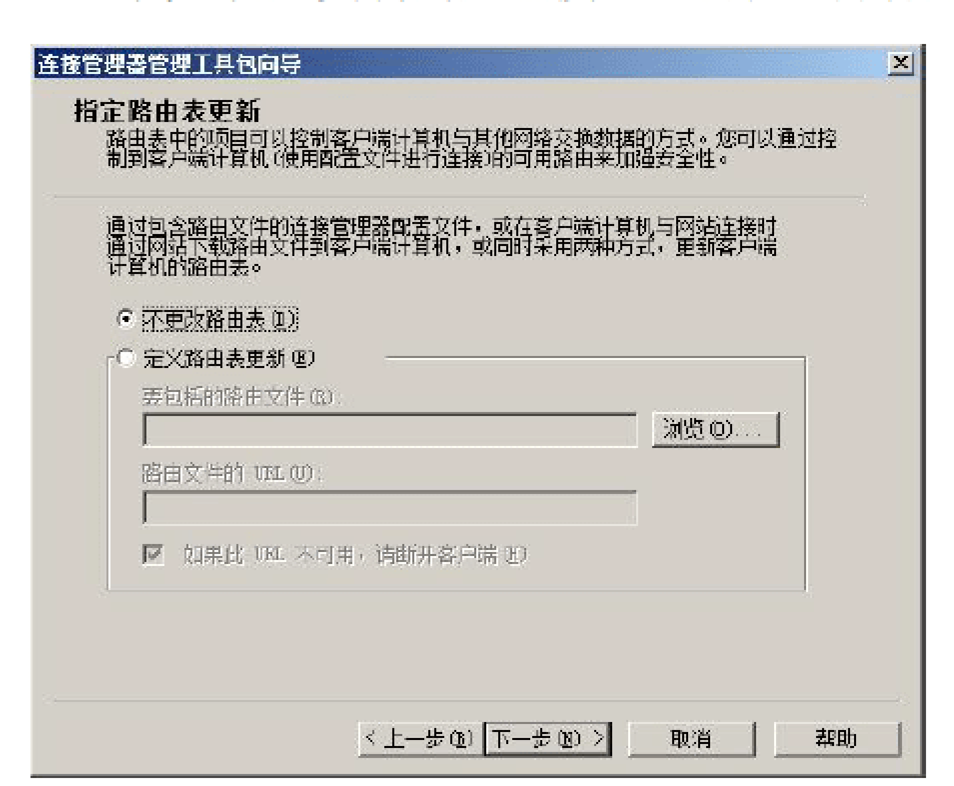


图 11-67 “指定路由表更新”界面

图 11-68 “配置 Internet Explorer 的代理设置”界面

⑮ 单击“下一步”按钮，显示如图 11-69 所示的“添加自定义操作”界面，根据需要配置自定义操作。

⑯ 单击“下一步”按钮，显示如图 11-70 所示的“显示自定义登录位图”界面。如果用户想要在登录对话框使用自定义位图，那么选择“自定义图形”单选按钮，然后指定位图的位置。

⑰ 单击“下一步”按钮，显示如图 11-71 所示的“显示自定义电话簿位图”界面。如果用户想要在电话簿对话框使用自定义位图，那么选择“自定义图形”单选按钮，然后指定位图文件的位置。

⑱ 单击“下一步”按钮，显示如图 11-72 所示的“显示自定义图标”界面。如果用户想要在“网络和共享中心”或“网络连接”文件夹中使用自定义位图，则选择“自定义图标”单选按钮，并指定位图文件的位置。

⑲ 单击“下一步”按钮，显示如图 11-73 所示的“包括自定义帮助文件”界面。如果用户想要配置文件

中包含自定义帮助文件，则选择“使用此自定义帮助文件”单选按钮，并指定 CHM 文件的位置。

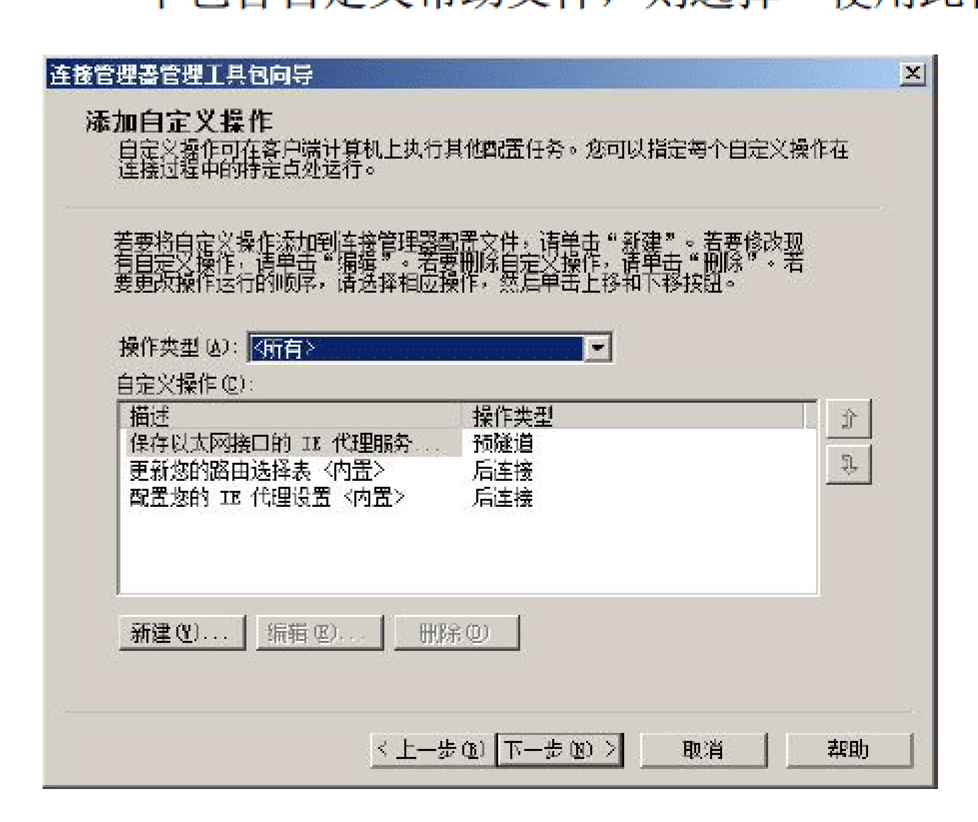


图 11-69　“添加自定义操作”界面



图 11-70　“显示自定义登录位图”界面



图 11-71　“显示自定义电话簿位图”界面



图 11-72　“显示自定义图标”界面

⑳ 单击“下一步”按钮，显示如图 11-74 所示的“显示自定义支持信息”对话框，如果用户想要在登录对话框中包含标准支持文本，则在“支持信息”文本框中，输入需要的文件。

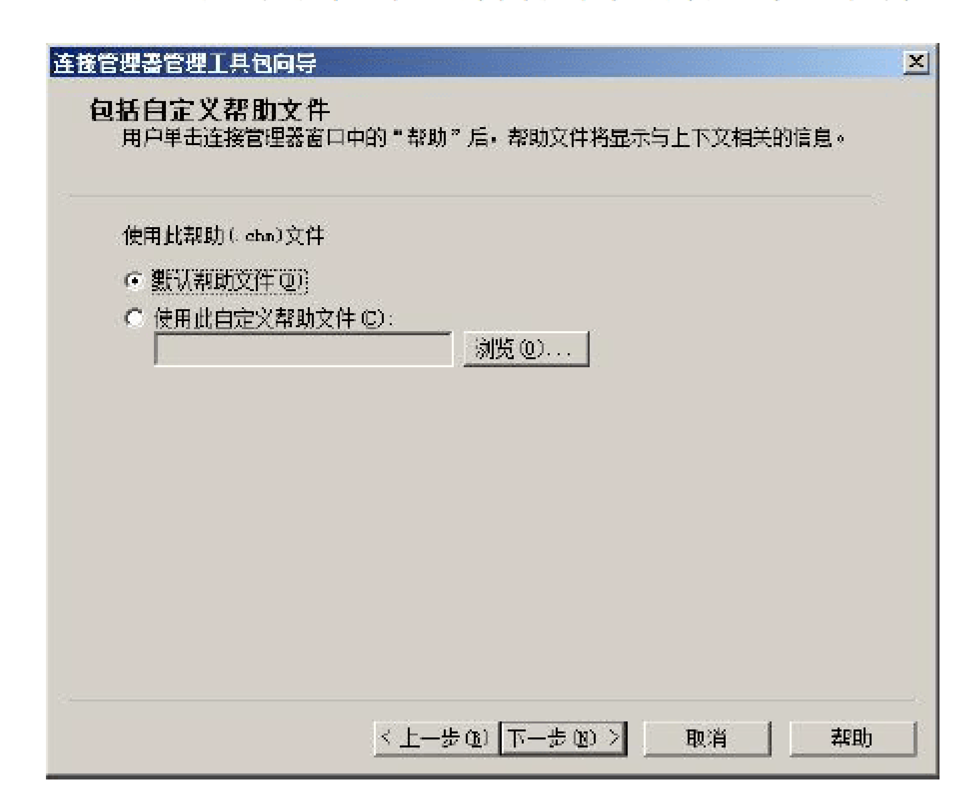


图 11-73　“包括自定义帮助文件”界面

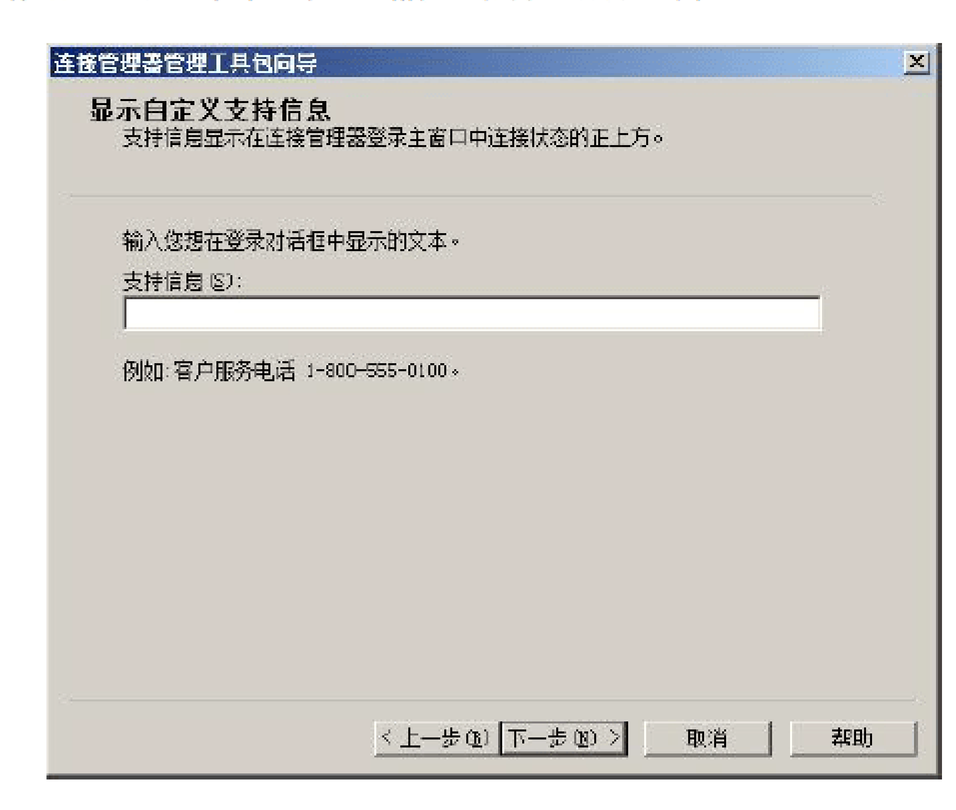


图 11-74　“显示自定义支持信息”界面

㉑ 单击“下一步”按钮，显示如图 11-75 所示的“显示自定义许可协议”界面。如果用户想要在 CM 配置文件安装过程中显示自定义许可协议，则指定包含许可协议文本的文件即可。

㉒ 单击“下一步”按钮，显示如图 11-76 所示的“使用连接管理器配置文件安装其他文件”界面，如果在安装配置文件的过程中包含 CM 配置文件的其他文件，则一一指定其位置即可。

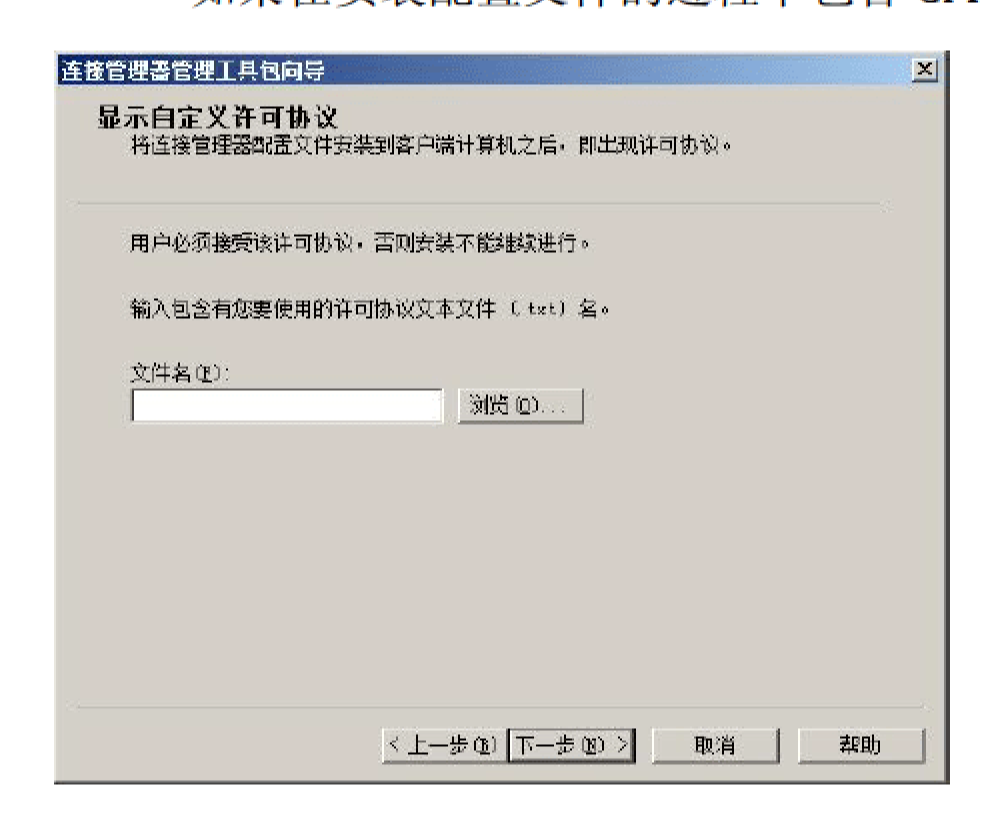


图 11-75 “显示自定义许可协议”界面

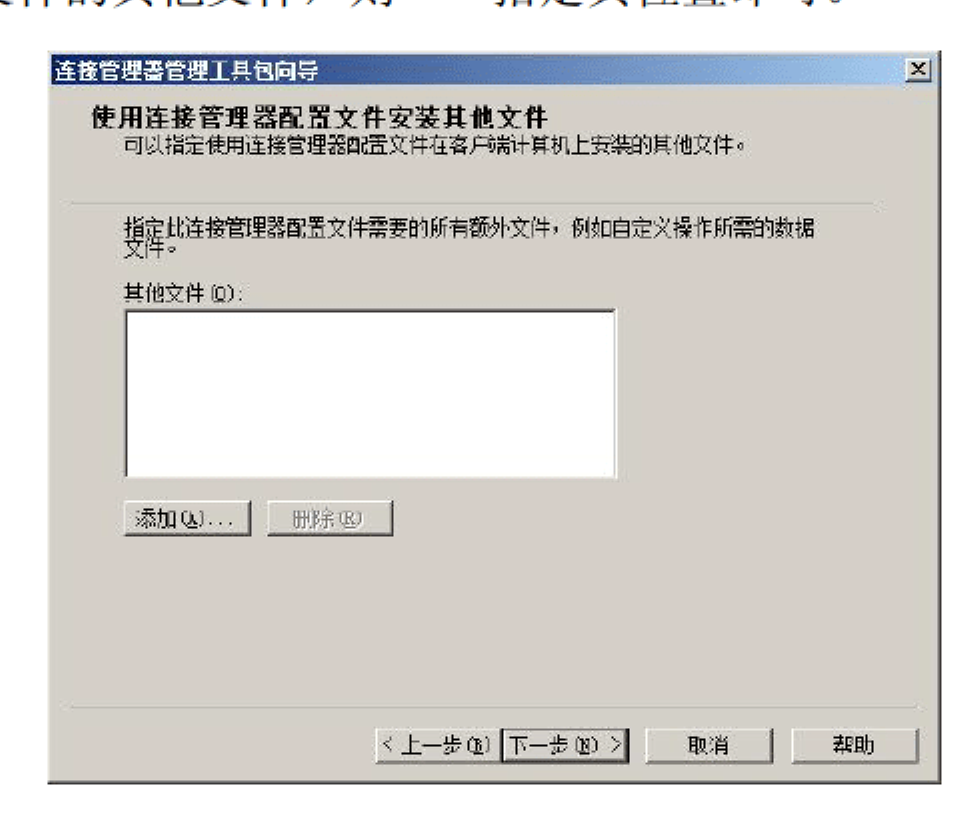


图 11-76 “使用连接管理器配置文件安装其他文件”界面

㉓ 单击“下一步”按钮，显示如图 11-77 所示的“构建连接管理器配置文件及其安装程序”界面。通常情况下，无需选中“高级自定义”复选框进行高级选项设置。

㉔ 单击“下一步”按钮，显示如图 11-78 所示的“连接管理器配置文件已完成，可以分发”界面，单击“完成”按钮即可。

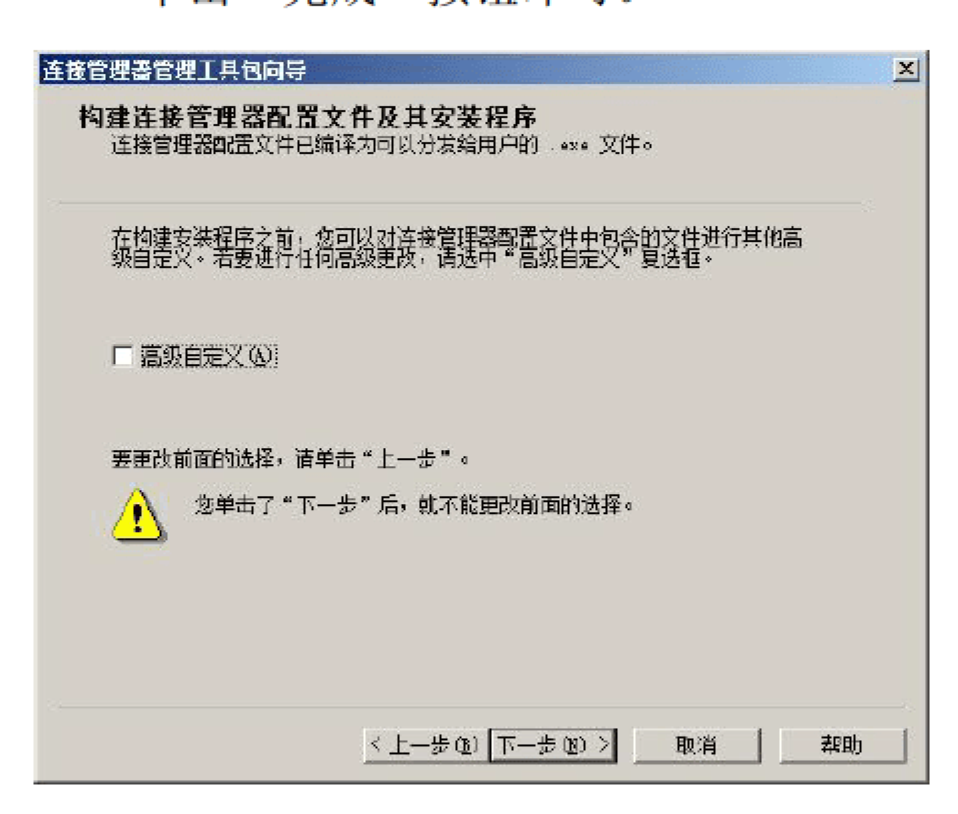


图 11-77 “构建连接管理器配置文件及其安装程序”界面

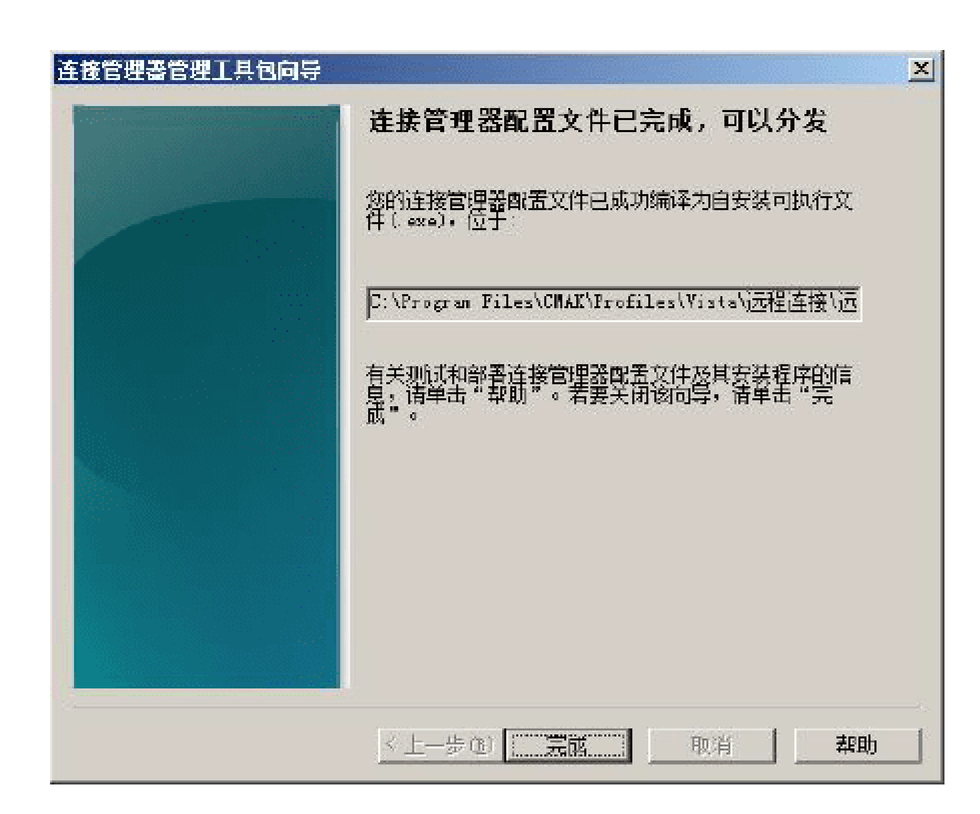


图 11-78 “连接管理器配置文件已完成，可以分发”界面

(3) 分发 CM 配置文件

管理员可以通过如下几种方法将 CM 配置文件分发到 VPN 客户端用户。

- 通过可移动存储介质分发，如光盘、U 盘等。这种方式花费较高，并且安全性较低。
- 通过 E-mail 分发 CM 配置文件。
- 通过下载分发 CM 配置文件。管理员可以将 CM 配置文件发布到 Web 或 FTP 服务器上，供用户下载。

第 12 章　站点对站点的 VPN 连接

站点对站点 VPN 连接的是两个分别独立的网络，相对于第 11 章介绍的远程访问 VPN 而言，功能更加强大，可以实现两个网络的安全互联。建立站点对站点的 VPN 连接后，局域网中的客户端可以通过 VPN 服务器，拨叫到对端网络中的任意客户端上。这种方式通常应用于大型企业网络不同分支之间的连接，既可以确保安全性，又不必花费高额的链路租金。管理员可以借助 Windows Server 2008 系统，或者网络中的路由器防火墙等设备实现点对点的 VPN 连接。

关键词

- 站点对站点 VPN 简介
- 点对点 VPN 连接的规划和设计
- 配置站点对站点 VPN 连接

12.1 站点对站点 VPN 简介

点对点 VPN 与远程访问 VPN 类似，同样支持多种加密协议和身份验证机制。不同的是在这种连接中没有客户端和服务器之分，两端负责建立 VPN 连接的 VPN 服务器均称为 VPN 路由器。在 Windows Server 2008 中有两种类型的站点对站点 VPN 技术。

- 点对点通道协议(PPTP)：PPTP 使用用户级的点对点协议(PPP)身份验证方式和微软点对点加密(MPPE)进行数据加密。
- 使用 Internet 协议安全的第二层通道协议(L2TP/IPSec)：L2TP/IPSec 使用用户级的点对点协议(PPP)身份验证方式，以及 IPSec 进行计算机级的 IPSec 身份验证和数据验证、完整性验证和加密。

12.1.1 点对点 VPN 的实现机制

建立站点对站点 VPN 连接的 VPN 路由器也叫呼叫路由器；监听入站站点对站点连接的 VPN 路由器也叫应答路由器。在连接过程中，呼叫路由器验证应答路由器，身份验证方式支持彼此认证，应答路由器验证呼叫路由器。

默认情况下，站点到站点 VPN 连接是请求拨号连接，只有当网络流量必须通过此接口转发(需要转发 IP 数据包到对应的远程网络)时才建立连接。此时呼叫路由器(VPN 客户端)初始化这个连接，应答路由器(VPN 服务器)侦听连接请求，接收来自呼叫路由器的连接请求，根据请求建立连接，并且在空闲一定时间(默认为 5min)后断开连接。可以配置连接为永久连接方式。此时，VPN 服务器会保持此连接的连接状态，如果连接中断则立即重新初始化连接。

为了避免呼叫路由器建立不需要的连接，可以按照以下两种方式来限制呼叫路由器建立请求的站点到站点 VPN 连接：

- IP 请求拨号筛选器。可以使用请求拨号筛选来决定哪种类型的 IP 流量不能导致请求拨号连接的建立，也可以配置哪种类型的 IP 流量可以导致连接的建立。配置请求拨号筛选的方法是：在“路由和远程访问”控制台的“网络接口”窗口中，右击请求拨号接口，再单击“IP 请求拨号筛选器”选项，进行相应设置即可。
- 拨出时间。可以使用拨出时间来配置允许或禁止呼叫路由器建立站点到站点 VPN 连接的时间段。配置拨出时间的方法是，在“路由和远程访问”控制台的“网络接口”窗口中，右击请求拨号接口，选择“拨出时间”选项，设置拨出时间即可。还可以使用远程访问策略，配置允许传入请求拨号路由连接的时间。

12.1.2 请求拨号路由概述

Windows Server 2008 路由和远程访问服务，支持基于拨号连接的请求拨号路由、VPN 连接以及基于以太网的 PPP 连接。请求拨号路由与远程访问不同，远程访问只连接单一计算机到网络上，请求拨号路由连接网络的两部分。正如执行路由和远程访问一样，远程访问和请求拨号连接可以分别启动或一起启动，共享如下属性：

- 用户账户拨号属性的行为。
- 安全(身份验证协议和加密)。
- 使用 Windows 或 RADIUS 进行身份验证、授权和记账。
- 使用网络策略进行授权。
- IPv4 地址分配和配置。
- 检修设备，包括事件日志，Windows 或 RADIUS 身份验证和记账日志，以及追踪。

1. 请求拨号路由更新

通常路由协议依靠周期广播过程进行路由信息通信。例如，RIP 路由协议每隔 30s 就在所有接口上广播路由表的内容。对于敏感的拨号 Internet 连接，这种周期性的行为可能导致路由器每隔 30s 就呼叫其他路由器，从而引起不必要的路由开销。

如果不希望使用路由协议更新 VPN 路由器的路由表，则必须添加静态路由。对应 IPv4 或 IPv6 地址前缀的静态路由可以手动或者自动配置。对请求拨号接口自动插入 IPv4 静态路由也叫做自动更新。自动静态更新的请求拨号接口会发送 RIP 请求，到另一端的所有路由器的路由表中。根据请求的回应，被请求路由器的 IPv4 路由作为静态路由自动添加到发出请求路由器的路由表中。

静态路由是持续的；即使连接断开或路由器重启，它们仍然保持在路由表中。自动静态更新是一次性、单向的路由消息交换。

2. 即时连接和持久连接

站点对站点 VPN 连接的时效性包括即时连接和持久连接两种：

- 当通信必须通过连接转发，并且连接还没有建立时，创建即时站点对站点连接。连接可以通过配置呼叫路由器的静态路由建立请求拨号连接来进行创建。当匹配路由的通信必须转发时，连接创建，并且通信被转发。即时连接在到达设置时间后终止。
- 持久站点对站点 VPN 连接总是保持连接状态。如果连接断开，将会立即重试。



提示：默认情况下，请求拨号接口使用带有 5min 停机超时的即时连接。

3. 约束即时连接的建立

为了防止呼叫路由器建立不必要的即时连接，用户可以通过如下方式约束呼叫路由器建立站点对站点 VPN 连接：

- 请求拨号筛选。用户可以使用请求拨号筛选来配置不会导致请求拨号连接建立的 IPv4 或 IPv6 通讯的类型，或者导致连接建立的 IPv4 或 IPv6 通讯的类型。
- 拨号超时。用户可以使用拨号超时配置呼叫路由器被允许或者不允许建立站点对站点 VPN 连接。
- 网络策略。当入站请求拨号连接在应答路由器上被允许时，用户也可以使用网络策略配置 VPN 连接时间。

12.1.3　点对点 VPN 的类型

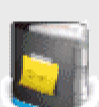
站点到站点 VPN 连接可以分为两种类型：单向初始化连接和双向初始化连接。

1. 单向初始化连接

在单向初始化连接中，一台 VPN 路由器总是担任呼叫路由器(类似于远程访问 VPN 中的 VPN 客户端)，而另一台 VPN 路由器总是担任应答路由器(VPN 服务器)。当单向初始化的站点到站点连接成功创建后，呼叫路由器上将添加到达应答路由器所属专用网络的路由，但是应答路由器上不会添加到达呼叫路由器所属专用网络的路由。此时，应答路由器不能访问呼叫路由器所属的专用网络，因此通常情况下较少使用单向初始化连接。

单向初始化的连接需要满足下列条件：

- 应答路由器被配置为局域网和请求拨号路由器。
- 在应答路由器上为呼叫路由器的身份验证凭据添加用户账户。
- 在应答路由器上配置了请求拨号接口，并且其名称与呼叫路由器所使用的用户账户名称相同。



提示：请求拨号接口不是用于拨号的，因此没有配置呼叫路由器的主机名或 IP 地址，也没有配置有效的拨出用户身份验证信息。

- 如果建立 L2TP/IPSec 模式的站点到站点 VPN 连接，还需要在呼叫路由器上安装客户端身份验证证书，在应答路由器上安装服务器身份验证证书；如果不安装证书，则需要配置预共享的 IPSec 密钥。

2. 双向初始化连接

双向初始化连接可以视为两个方向上的单向初始化连接，每个 VPN 路由器同时是呼叫路由器和应答路由器，可向对方进行连接初始化和接受对方的站点到站点 VPN 连接请求。当站点到站点连接成功创建后，每个 VPN 路由器上均会添加到达对方路由器所属专用网络的路由，从而各自的专用网络可以访问远端网络。

双向初始化的站点到站点 VPN 连接需要满足下列条件：

- 两个路由器都被配置为 LAN 和请求拨号路由器。
- 在每个路由器上为对端路由器的身份验证凭据添加了用户账户，并且配置了名称与呼叫路由器所使用的用户账户名称相同的请求拨号接口。
- 如果采用 L2TP/IPSec 模式的站点到站点 VPN 连接，还需要在每个路由器上同时安装客户端身份验证证书和服务器身份验证证书；如果不安装证书，则需要配置欲共享的 IPSec 密钥。

在部署站点到站点 VPN 服务之前，用户需要配置 VPN 服务器提供远程访问 VPN 服务，本地 VPN 服务器会将远端 VPN 服务器发起的站点到站点 VPN 连接请求，视为一个普通 VPN 客户端计算机发起的远程访问 VPN 连接请求，并进行相应的处理。

远程访问客户端和请求拨号路由器都可以初始化一个 VPN 连接，当远程访问客户端和请求拨号路由器向 VPN 服务器初始化 VPN 连接时，它们所发送的身份验证信息中包含用于初始化连接的用户名。如果响应这个连接请求的 VPN 服务器(应答路由器)上具有和此用户名一致的请求拨号接口，则此连接就是请求拨号连接；否则，传入的连接就是远程访问连接。

12.1.4 Windows 站点对站点 VPN 的组件

基于 Windows Server 2008 系统实现的站点对站点 VPN 连接，大致结构如图 12-1 所示。

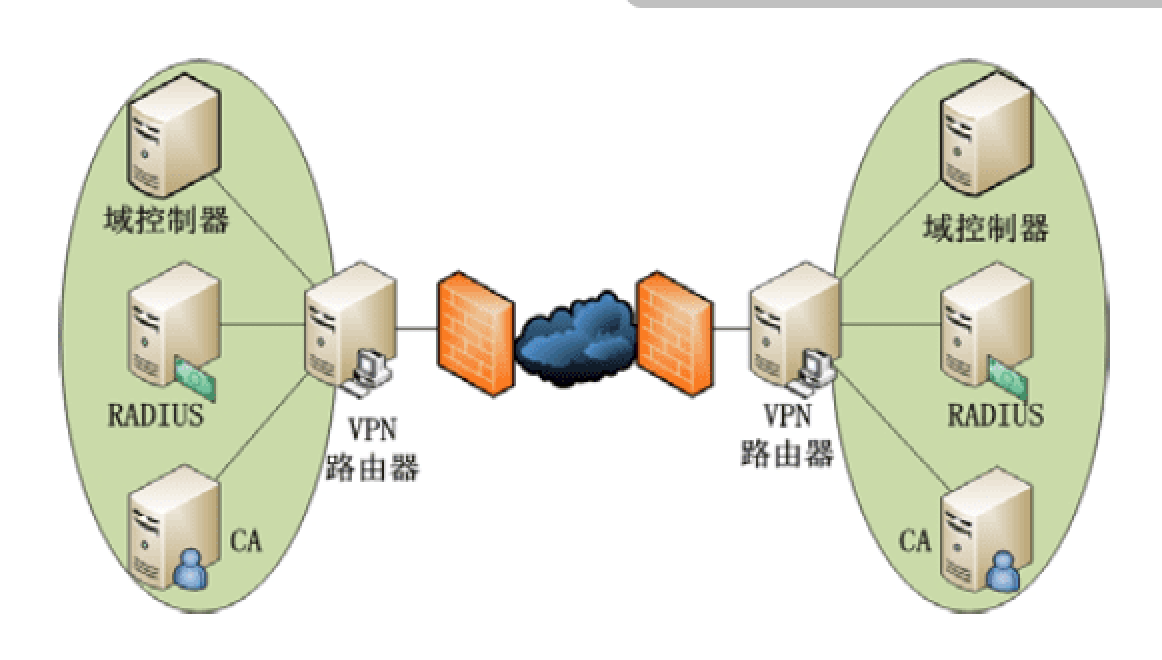


图 12-1　基于 Windows 的站点对站点 VPN 的组件

图 12-1 显示了基于 Windows 的站点对站点 VPN 的组件。

基于 Windows 的站点对站点 VPN 的组件如下：

- VPN 路由器。VPN 路由器或者建立站点对站点 VPN 连接到应答路由器，并且通过基于 VPN 请求拨号连接转发数据包，或者监听站点对站点 VPN 连接尝试，强制身份验证和连接要求，并且通过基于的 VPN 请求拨号连接转发数据包。
- RADIUS 服务器。RADIUS 服务器为应答路由器、远程访问 VPN 服务器和其他类型访问服务器的网络访问尝试提供集中身份验证和授权记账功能。
- 活动目录域控制器。活动目录域控制器验证身份验证的证书，并提供用户账户信息评估应答路由器的授权。
- CA 服务器。CA 是 PKI 的一部分，负责发布呼叫路由器的用户或计算机证书和应答服务器的计算机证书，以及站点对站点 VPN 连接的身份验证的 RADIUS 服务器。

12.2　点对点 VPN 连接的规划和设计

点对点的 VPN 连接功能比较强大，对实施过程中的每个环节要求都非常严格。安全级别需求较低的用户，则可以只配置双方的 VPN 路由器和内网路由即可。如果用户需求的安全级别较高，则仍需要配置相应的身份验证机制，如数字证书等。

12.2.1　VPN 协议

在点对点模式的 VPN 连接中，Windows Server 2008 系统允许使用 PPTP 和 L2TP/IPSec 协议，有关该协议的详细内容，可参考本书第 11 章中的相关介绍。

12.2.2　身份验证方式

为了认证尝试 VPN 连接的呼叫路由器，Windows Server 2008 支持广泛的身份验证协议，例如 MS-CHAP v2 和 EAP-TLS：

- MS-CHAP v2 是一种基于密码的身份验证方式，提供彼此的身份验证。
- EAP-TLS 是一种基于证书的身份验证方式，与 PKI 联合使用。EAP-TLS 也提供彼此的身份验证。对于 EAP-TLS，呼叫路由器发送用户证书进行身份验证，并且验证服务器也发送计算机证书进行

身份验证。

1. 身份验证协议的设计选择

如果用户拥有 PKI，建议站点对站点 VPN 连接使用 EAP-TLS。如果没有配置 PKI 或者不具备 PKI，则可以使用 MS-CHAP v2。EAP-TLS 比 MS-CHAP v2 更安全，不依赖于密码，并且可以防御离线字典攻击。

2. 身份验证协议的要求

对基于加密的 PPTP 连接，用户必须使用 EAP-TLS 或 MS-CHAP v2。只有这些身份验证协议可以提供产生预会话初始化加密密钥的机制。EAP-TLS 要求 PKI 发布用户和计算机证书。

3. 注意事项

在点对点 VPN 连接中，选择身份验证方式时应注意如下事项：

- 如果用户必须使用基于密码的 MS-CHAP v2，则需要在网络中使用强密码。强密码至少为 8 个字符，且包含大小写字母、数字和标点符号。
- 对于 EAP-TLS，呼叫路由器默认情况下验证应答路由器的计算机证书。
- 对于基于 L2TP/IPSec 的连接，任何用户级的身份验证协议都可以使用，因为身份验证发生在 VPN 路由器建立 IPSec 保护通道之后。推荐使用 EAP-TLS 或 MS-CHAP v2，来提供有效的用户身份验证和彼此身份验证。

12.2.3 VPN 路由器

VPN 路由器建立或接受基于 VPN 的请求拨号连接。在整个连接过程中，呼叫路由器需要完成如下工作：

- 根据连接持久性、管理员动作或数据包被转发的时间建立 VPN 连接。
- 在转发数据包前等待身份验证和授权。
- 作为路由器，在自己站点的节点和应答路由器的站点节点之间转发数据包。

应答路由器需要完成如下工作：

- 监听 VPN 连接尝试。
- 在允许数据传输之前进行身份验证和授权 VPN 连接。
- 作为路由器，在自己站点的节点和呼叫路由器的站点节点之间转发数据包。

1. 配置路由和远程访问

双方站点的 VPN 路由器都是借助“路由和远程访问”配置向导完成的，开始阶段双方操作完全相同。详细配置过程，可参照本书第 11 章中的相关介绍。

2. VPN 路由器的设计

规划和设计 VPN 路由器时应遵循如下原则：

- VPN 路由器可以配置为从 DHCP 获取 IPv4 地址，或者从手动配置的地址范围中获取 IPv4 地址。使用 DHCP 获取 IPv4 地址简化了配置；但是，用户必须确保 VPN 路由器所在子网的 DHCP 范围，拥有足够的地址分配给所有物理连接子网的计算机和最大数量的远程访问客户端。
- 应答路由器可以评估身份验证和 VPN 连接的授权，或者依赖 RADIUS 服务器。当配置应答路由器时，用户可以为身份验证或记账选择使用 Windows 或 RADIUS。

- 如果 RADIUS 服务器是运行 Windows Server 2008 的计算机和网络策略服务器(NPS)，则其必须是活动目录域的成员。
- “路由和远程访问服务器安装向导”不能为远程访问 VPN 连接自动启用 IPv6 支持。
- 对于即时连接，如果用户想要防止在特定时间或对特定类型通讯建立连接，应配置拨号超时或请求拨号筛选器。

12.2.4 Internet 基础结构

若想实现呼叫路由器到应答路由器的正常通信，首先必须确保应答路由器的 DNS 名称或 IP 地址是可以到达的，其次双方的 VPN 路由器必须允许 VPN 通讯进出站。

1. 应答路由器名称的可解析性

在呼叫路由器的请求拨号接口中，用户都是通过 FQDN 来引用应答路由器的，而非 IPv4 或 IPv6 地址。只要 FQDN 名称可以解析为 IPv4 或 IPv6 地址，用户就可以使用 FQDN。所以，用户必须确保当配置 VPN 连接时，应答路由器所使用的名称可以解析为 DNS 服务器所使用的 IPv4 或 IPv6 地址。

2. 应答路由器的可到达性

为了确保可到达性，应答路由器必须分配一个公有 IPv4 地址或者全局 IPv6 地址。如果被分配一个静态公有 IPv4 地址或全局 IPv6 地址前缀，通常情况下不会出现问题。在一些 IPv4 配置中，应答路由器实际上使用专有 IPv4 地址配置，并且拥有公有的静态 IPv4 地址。在 Internet 和应答路由器之间的设备将应答路由器的公有和有效 IPv4 地址转换为数据包发送到应答路由器。

尽管路由基础结构可能提供可到达性，但是应答路由器可能由于防火墙、数据包筛选器路由器、NAT、安全网关或其他类型设备的设置，而无法到达。

12.2.5 站点网络基础结构

站点的网络基础结构是 VPN 设计的重要元素。如果没有适当的内网基础结构设计，VPN 路由器就无法正常工作。例如，无法解析内网主机名称、无法获取内网可到达的 IPv4 地址或 IPv6 子网前缀等。

1. 内网名称解析

如果呼叫路由器使用 DNS 或 WINS 服务器的 IP 地址进行配置，那么 DNS 和 WINS 服务器的 IPv4 地址将不能在 PPP 连接协商过程中从应答路由器请求。如果呼叫路由器没有使用 DNS 或 WINS 服务器的 IP 地址进行配置，那么 DNS 和 WINS 服务器将被请求。应答路由器不会从呼叫路由器请求 DNS 或 WINS 服务器的 IPv4 地址。

与基于 Windows 的远程访问客户端不同，呼叫路由器不会发送 DHCP 请求消息到应答路由器，来获取其他 TCP/IP 配置消息。

默认情况下，呼叫路由器不会使用从应答路由器获得的 DNS 或 WINS 服务器注册自己。为了更改该行为，设置注册表值 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\PPP\ Control-Protocols\BuiltIn\RegisterRoutersWithNameServers 为 1。

2. 路由到内网的 VPN 路由器

每台 VPN 路由器都是一个 IPv4 或 IPv6 路由器，必须使用 IPv4 或 IPv6 路由进行适当的配置，使得 Internet 上所有位置和 VPN 路由器站点都可到达。每台 VPN 路由器需要进行如下配置：

- 指向防火墙或路由器直接连接 Internet 的默认路由，使用户可以到达 Internet 上的所有位置。
- 概括了 VPN 路由器站点的所有 IPv4 或 IPv6 地址空间的一条或多条路由，使 VPN 路由器站点的所有路由从 VPN 路由器都可到达。如果没有这些路由，则没有连接到相同子网的 VPN 路由器的节点不可到达。

管理员可以通过如下两种方式为 VPN 路由器分配 IPv4 地址。

- On-subnet address range：VPN 路由器所属内网子网的地址范围。
- Off-subnet address range：VPN 路由器逻辑所属的不同子网的地址范围。

如果使用 On-subnet address range 方式，则不需要配置其他路由，因为 VPN 路由器可以作为 VPN 路由器的所有数据包的 ARP 代理。站点子网的路由器和主机转发数据包到 VPN 接口，然后 VPN 路由器再转发到 VPN 路由器。

如果使用 Off-subnet address range 方式，则用户必须添加概括子网地址范围的路由到子网路由基础结构中，保证 VPN 路由器的通讯被转发到 VPN 路由器，然后从 VPN 路由器转发到适当的 VPN 路由器。为了提供路由地址范围的最好概括，应选择可以使用单一前缀和子网掩码表示的地址范围。

为了添加概括子网地址范围的路由到站点路由基础结构中，应添加静态路由到 VPN 服务器的相邻路由器中。配置相邻路由器传播该静态路由到使用动态路由协议的站点中的其他路由器上。

如果内网包含单独的子网，用户必须为子网地址范围的持续路由配置每个站点主机，或者使用 VPN 路由器作为默认网关配置每个站点主机。所以，对包含单独子网的 SOHO 网络推荐使用 On-subnet address range 池。



注意：建议使用 On-subnet address range 方式手动配置 VPN 路由器，通过 DHCP 获取 IPv4 地址或者手动配置 On-subnet 地址池。

12.2.6 身份验证基础结构

在点对点的 VPN 连接中，身份验证环节主要包括认证呼叫路由器的数字证书、授权 VPN 连接、记录 VPN 连接的创建和终止以及确认用户账户的真实身份等。基本验证基础结构主要是 VPN 路由器本身、RADIUS 服务器或域控制器。

1. 为身份验证使用 Windows 或 RADIUS

基于 Windows Server 2008 的 VPN 路由器可以配置使用 Windows 或 RADIUS 来进行身份验证或记账。具体应用和配置过程与远程访问 VPN 完全相同，用户可以参考本书第 11 章中的相关介绍。

2. 域用户账户和组

活动目录域包含路由和远程访问或 NPS 所使用的用户账户和组，进行认证和授权 VPN 连接尝试。用户账户包含用户名和用户密码的加密形式，用于验证呼叫路由器的用户证书。此外账户属性决定了用户账户是否启用、锁定或允许登录。如果用户账户被禁用、锁定或只允许在特定时间登录，那么站点对站点 VPN

连接尝试将被拒绝。

请求拨号路由器必须能够按需连接，不需要人工干涉，所以呼叫路由器的用户账户必须在“账户”选项卡中的账户属性对话框中进行配置。确保取消选中“用户必须在下次登录时更改密码”复选框，以及“密码不会过期”复选框已经选中。

用户应该为每台呼叫路由器使用独立的用户账户，每个用户账户应该拥有匹配应答路由器的请求拨号接口的用户名。

3. 注意事项

配置身份验证基础结构时应注意如下事项：

- 如果拥有多个 VPN 服务器和路由器，并且想要进行集中身份验证、授权和记账服务，则可以使用 RADIUS 进行身份验证和记账。
- 如果用户账户数据库为活动目录域服务，则可以使用 NPS 作为 RADIUS 服务器。
- 为了更好地管理远程访问 VPN 连接的授权，为 VPN 访问在活动目录中创建通用组，包含允许建立远程访问 VPN 连接的用户账户的通用组。

无论为本地或在 NPS 服务器上配置，都可以使用指定 VPN 的网络策略授权 VPN 连接，并且指定连接约束和要求。

12.2.7　PKI

为 L2TP 连接和使用 EAP-TLS 的站点对站点 VPN 连接执行基于证书的身份验证，证书机构必须在验证过程中发布适当的证书，并且验证提交的证书。

1. L2TP/IPSec 连接的计算机证书

点对点 VPN 连接中 L2TP/IPSec 连接的计算机证书，与远程访问 VPN 完全相同，详细内容可参考第 11 章中的相关介绍。

2. EAP-TLS 的 PKI

为站点对站点 VPN 连接执行 EAP-TLS 身份验证时，应满足下列要求：

- 呼叫路由器必须在 EAP-TLS 认证过程中使用用户证书配置。
- 认证服务器必须在 EAP-TLS 认证过程中使用计算机证书配置。

在下列条件满足时 EAP-TLS 身份验证成功：

- 呼叫路由器提交有效的用户证书，该证书由应答路由器信任的根 CA 的证书链中的 CA 发布。
- 认证服务器提交有效的计算机证书，该证书由呼叫路由器信任的根 CA 的证书链中的 CA 发布。

对于 Windows Server 2008 或 Windows Server 2003 CA，路由器证书是请求拨号连接的特殊类型的用户证书。路由器证书必须获取，并且映射到活动目录用户账户中。当呼叫路由器尝试 VPN 连接时，路由器证书在身份验证过程中发送。如果路由器证书有效，认证服务器可以确定适当的用户账户获取拨号属性。

3. 注意事项

在点对点的 VPN 连接中应用 PKI 时，应注意如下事项：

- 对于使用计算机证书进行身份验证的 L2TP/IPSec 站点对站点 VPN 连接，用户必须在每台呼叫路

由器和应答路由器上安装计算机证书。

- 为了认证使用 EAP-TLS 的 VPN 连接，呼叫路由器必须安装了用户证书，并且认证服务器必须安装了计算机证书。
- 对于 EAP-TLS 身份验证，呼叫路由器的用户证书要求如下。
  - 证书必须包含专有密钥。
  - 证书必须由企业 CA 发布或者映射到活动目录的用户账户。
  - 证书必须绑定到 NPS 服务器上的受信任的根 CA，并且在网络策略中为站点对站点 VPN 连接指定的任何检查不能失败。
  - 证书必须在增强密钥使用区域使用客户端身份验证进行配置。
  - 主题选择名称必须包含用户账户的 UPN。
- 对于 EAP-TLS 身份验证，应答路由器的用户证书要求如下。
  - 证书必须包含专有密钥。
  - 证书必须由企业 CA 发布或者映射到活动目录的用户账户
  - 证书必须绑定到 NPS 服务器上的受信任的根 CA。
  - 证书必须在增强密钥使用区域使用服务器身份验证进行配置。
  - 证书必须由加密服务提供商(CPS)配置。
- 证书主题选择名称必须包含服务器的 FQDN。

12.3 配置站点对站点 VPN 连接

只配置呼叫路由器和应答路由器即可快速实现站点到站点的 VPN 连接，但是默认情况下，双方都是采用基本的 Windows 身份验证方式，安全性难以保证。通常情况下，借助 Windows Server 2008 系统，建立一个安全可靠的点对点 VPN 连接，包括如下配置任务：

- 配置证书
- 配置 Internet 基础结构
- 配置用户账户和组的活动目录
- 配置 RADIUS 服务器
- 配置应答路由器
- 配置呼叫路由器
- 配置站点网络基础结构
- 配置站点间网络基础结构

12.3.1 配置 VPN 路由器证书

需要明确的是，VPN 路由器证书并非必需要素，它是为了提高 VPN 连接的安全性而配置的。当使用证书身份验证的 L2TP/IPSec 连接，或者基于用户证书的 EAP-TLS 身份验证 VPN 连接时，用户必须为每台 VPN 路由器配置相应的计算机证书或用户证书。计算机证书的颁发和安装与远程访问 VPN 完全相同，此处不复赘述。这里主要介绍 VPN 路由器用户证书的部署。用户证书必须能够获取并映射到呼叫路由器所在域中的用户账户。

1. 为呼叫路由器创建用户账户

用户可以通过使用“新建请求拨号接口向导”和“活动目录用户和组”节点来完成该工作，推荐使用“新建请求拨号接口向导”完成。详细操作过程可参考本章“配置呼叫路由器”中的相关内容。

2. 配置 Windows Server 2008 CA 发布路由器证书

打开“证书颁发机构”控制台窗口，展开 CA 名称，右击“证书模板”，依次选择“新建”→“要发布证书模板”命令，显示如图 12-2 所示的“启用证书模板”对话框。选中“路由器(脱机申请)”模板，单击“确定”按钮即可添加到“证书颁发机构”控制台的“证书模板”中。

3. 申请路由器(脱机申请)证书

① 登录应答路由器系统，在 IE 浏览器地址栏中，输入 CA 服务器的地址，例如：“http://211.82.218.251/certsrv”，按 Enter 键，显示如图 12-3 所示的页面。注意，如果证书服务器设置了其他身份验证方式，如 Active Directory 用户身份认证，则需要输入相关的用户名和密码方可登录。

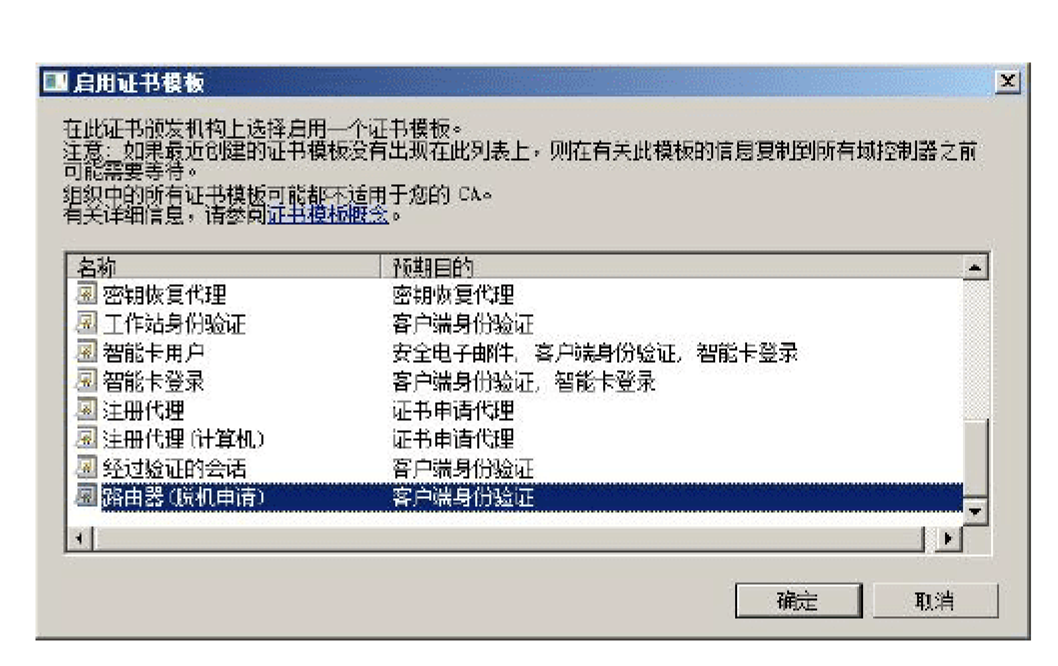


图 12-2　“启用证书模板”对话框



图 12-3　“欢迎使用”页面

② 单击“申请证书”超级链接，显示“申请一个证书”页面。继续单击“高级证书申请”超级链接，显示如图 12-4 所示的“高级证书申请”页面。

③ 单击“创建并向此 CA 提交一个申请”超级链接，显示“证书模板”页面。在证书模板区域，选择路由器(脱机申请)或者 CA 管理员检测到的模板名称，并输入用户名，如图 12-5 所示。在“密钥选项”选项区域中，选择“创建新密钥集”和“自动密钥容器名称”单选按钮。

④ 单击“提交”按钮，即可开始提交申请。相对于独立 CA 而言，企业 CA 可以立即响应用户申请证书的请求，并颁发证书。完成后显示如图 12-6 所示的“证书已颁发”页面。继续单击“安装此证书”超级链接，即可安装该证书。

4. 导出路由器(离线申请)证书为.CER 文件

① 打开 MMC 控制台，并添加本地计算机上的计算机证书控制单元。依次展开“个人”→“证书”节点，如图 12-7 所示。

② 右击通过 Web 方式申请的路由器(离线申请)证书，依次单击“所有任务”→“导出”命令，显示如图 12-8 所示的“欢迎使用证书导出向导”界面。

③ 单击“下一步”按钮，显示如图 12-9 所示的“导出私钥”界面，选择“不，不要导出私钥”单选

按钮。



图 12-4 “高级证书申请”页面

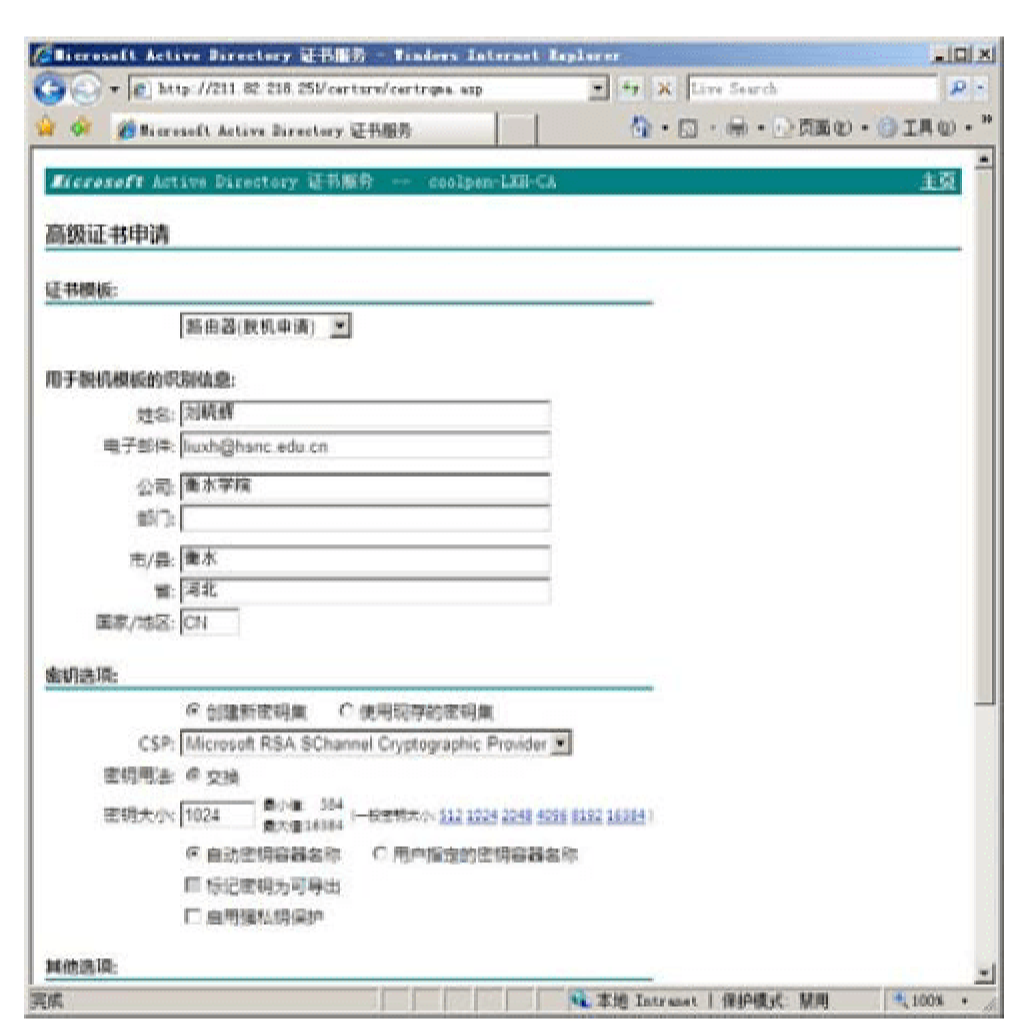


图 12-5 设置证书模板

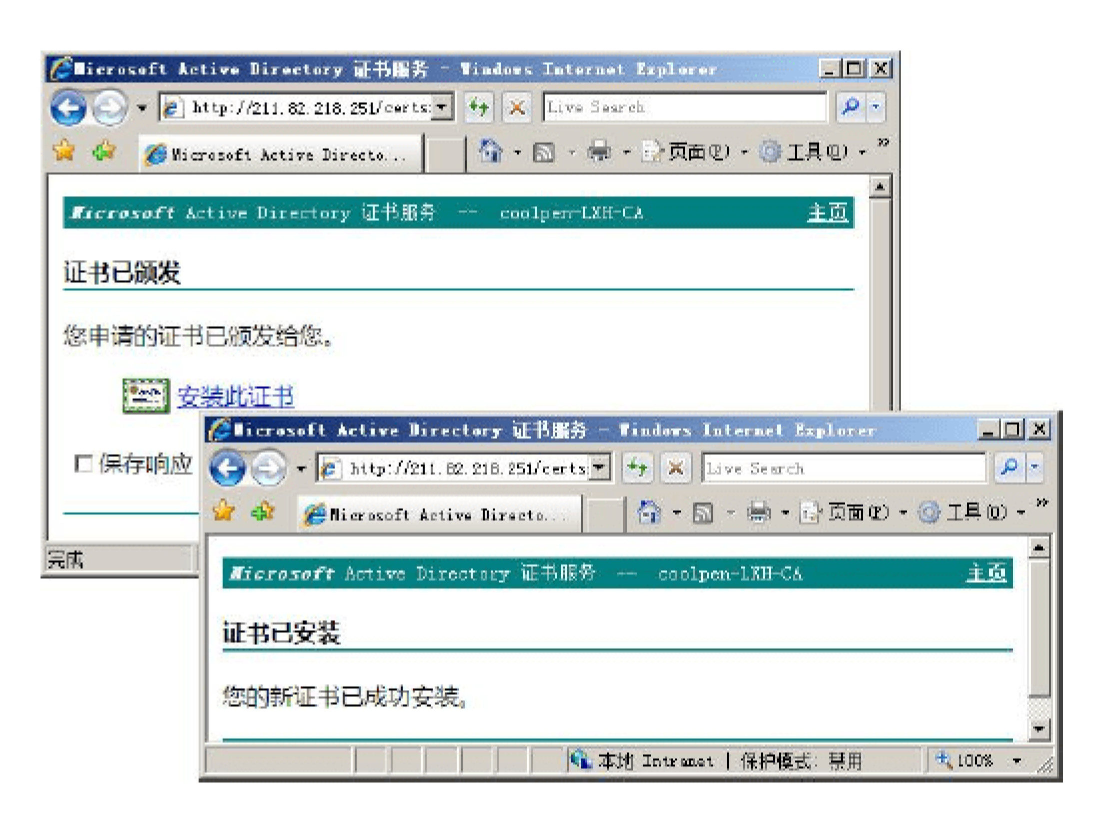


图 12-6 “证书已颁发”页面

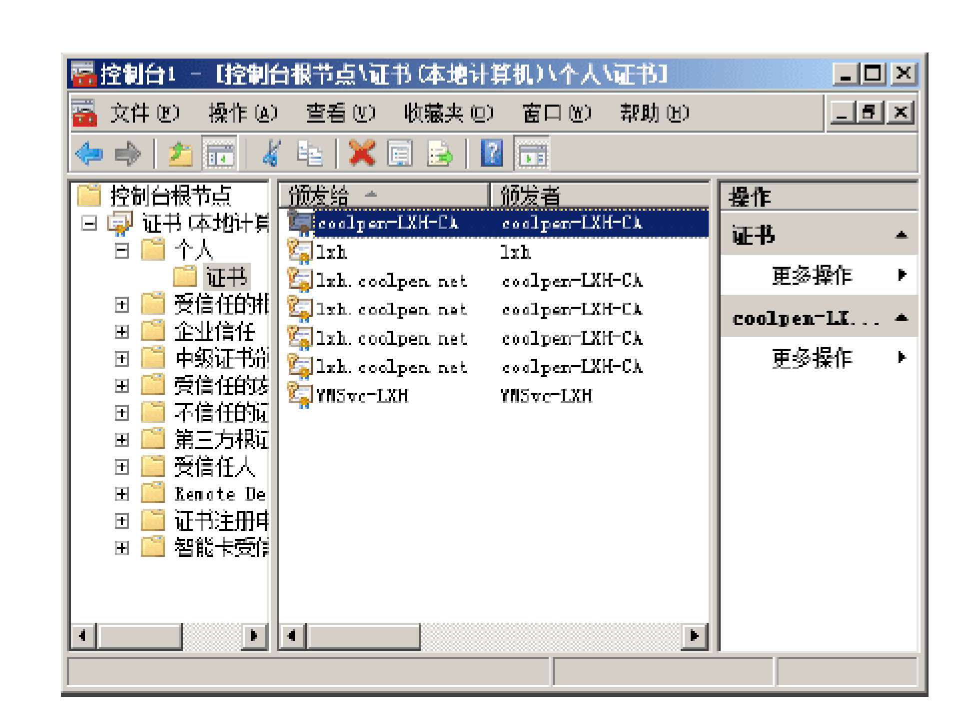


图 12-7 打开“证书”

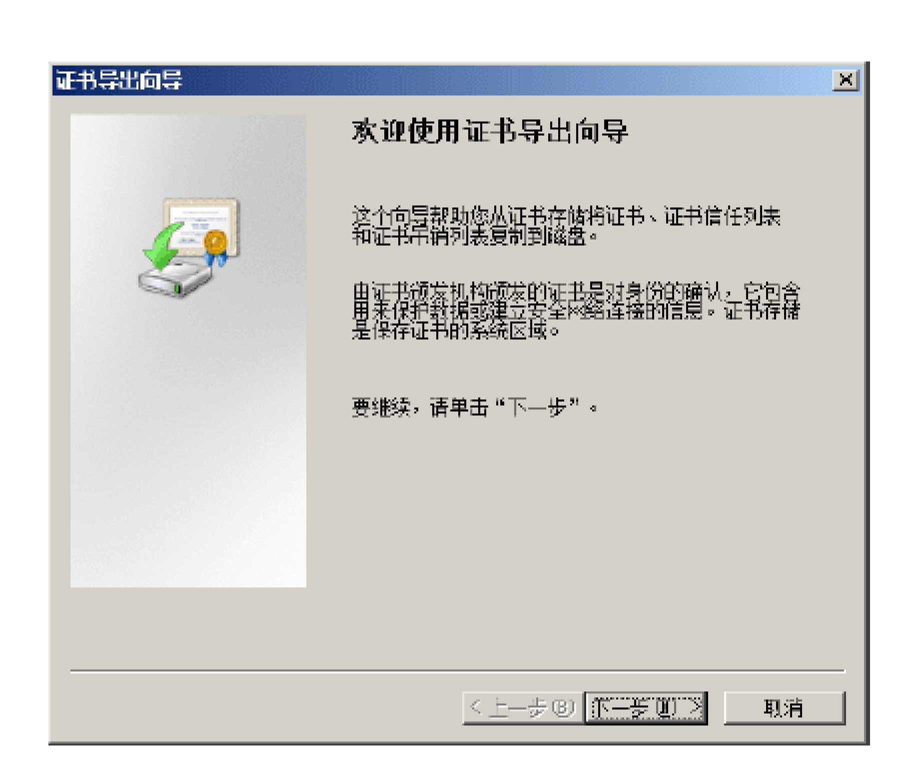


图 12-8 “欢迎使用证书导出向导”界面

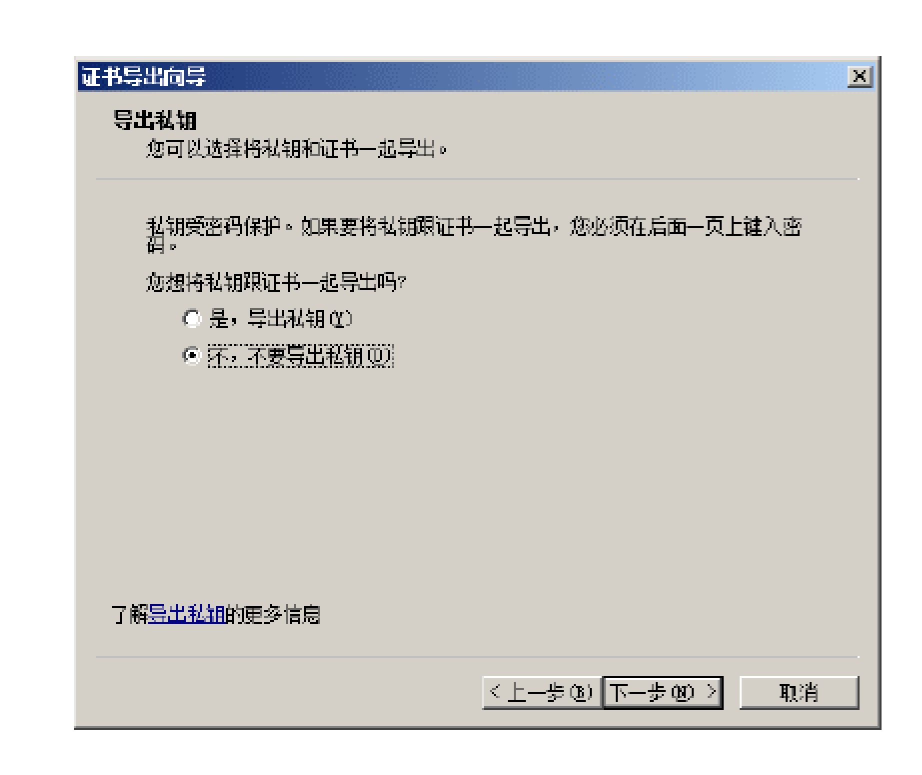


图 12-9 “导出私钥”界面

④　单击“下一步”按钮，显示如图 12-10 所示的“导出文件格式”界面，选择“DER 编码二进制 X.509(.CER)”作为导出文件格式。

⑤　单击“下一步”按钮，显示如图 12-11 所示的“要导出的文件”界面，设置证书文件的保存路径和文件名称。

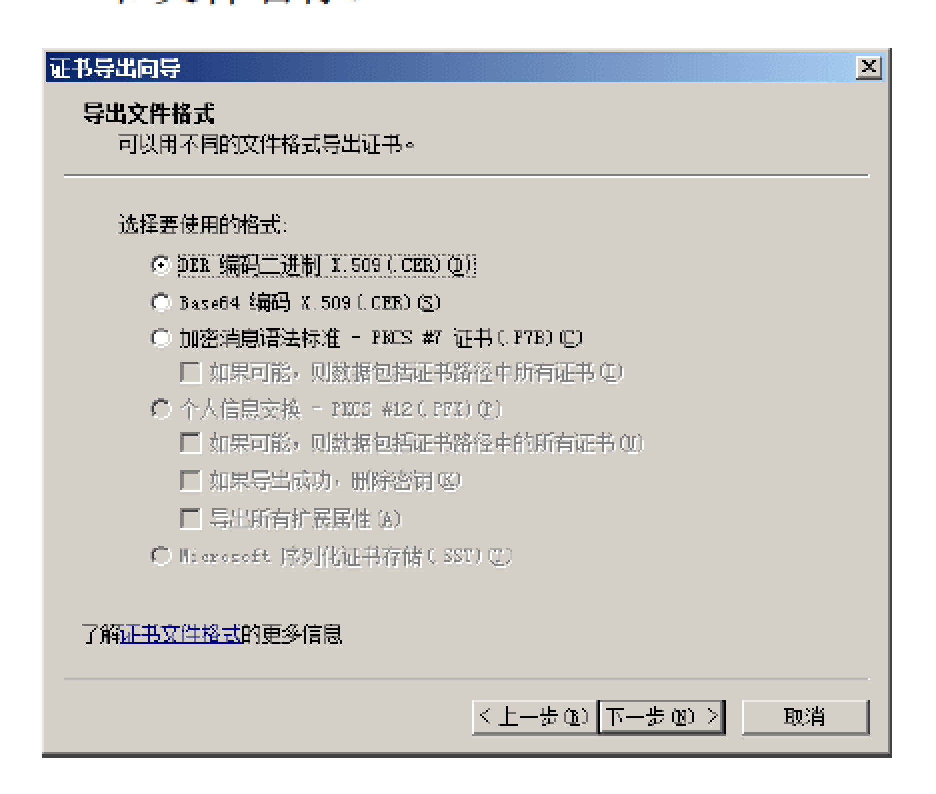


图 12-10　“导出文件格式”界面

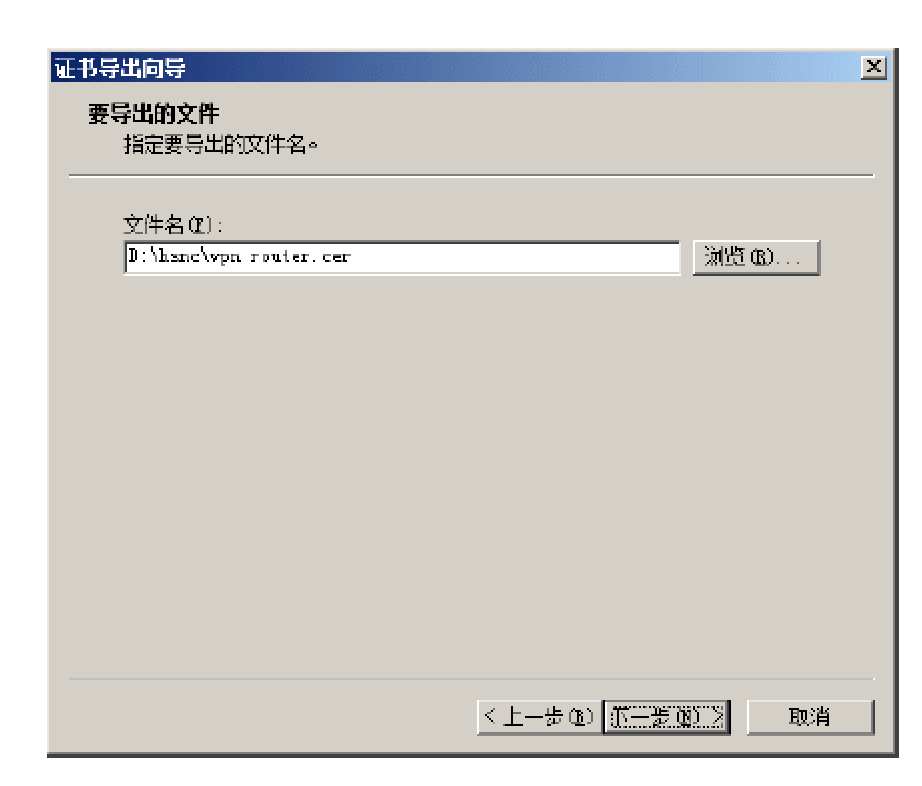


图 12-11　“要导出的文件”界面

⑥　单击“下一步”按钮，显示如图 12-12 所示的“正在完成证书导出向导”界面。

⑦　单击“完成”按钮，弹出如图 12-13 所示的“导出成功”提示框。

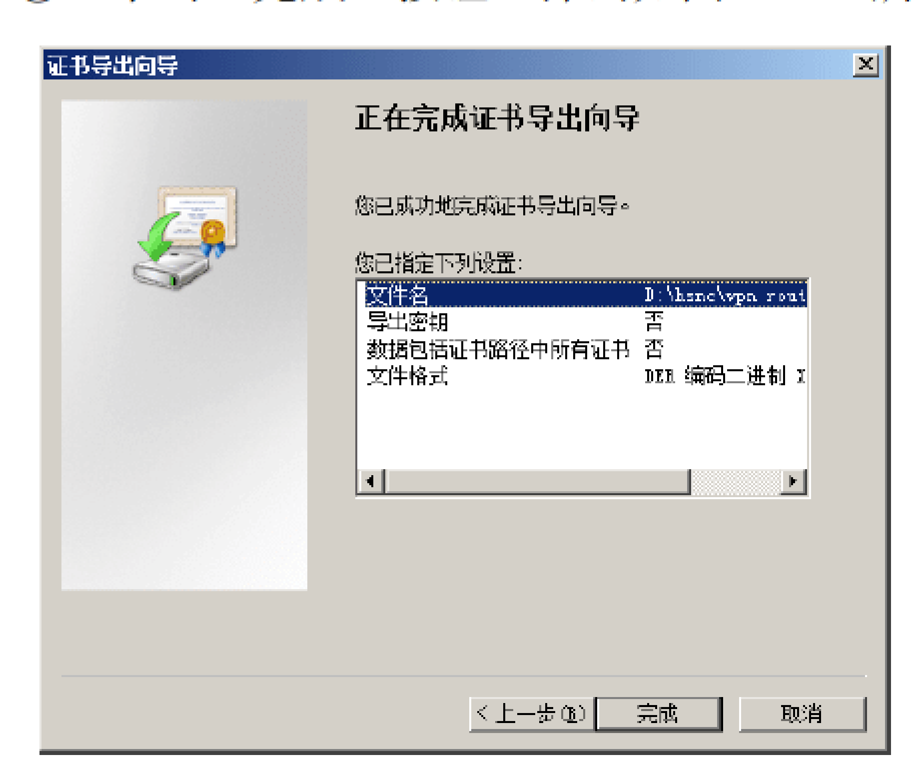


图 12-12　“正在完成证书导出向导”界面

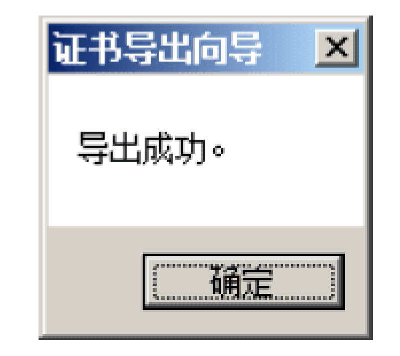


图 12-13　“导出成功”提示框

5. 映射.CER 证书文件到适当的用户账户

①　登录到域控制器，打开“Active Directory 用户和计算机”窗口，依次选择“查看”→“高级功能”命令，如图 12-14 所示。

②　展开被赋予呼叫路由器拨入权限的用户账户所在组织单位，右击用户账户或组，依次选择“所有任务”→“名称映射”命令，显示如图 12-15 所示的“安全身份映射”对话框。

③　在“X.509 证书”选项卡中，单击“添加”按钮，选择从 VPN 呼叫路由器上导出的.cer 证书文件，如图 12-16 所示。

④　单击“打开”按钮，显示如图 12-17 所示的“证书属性”界面，从中可以看到证书的颁发者以及主题信息。

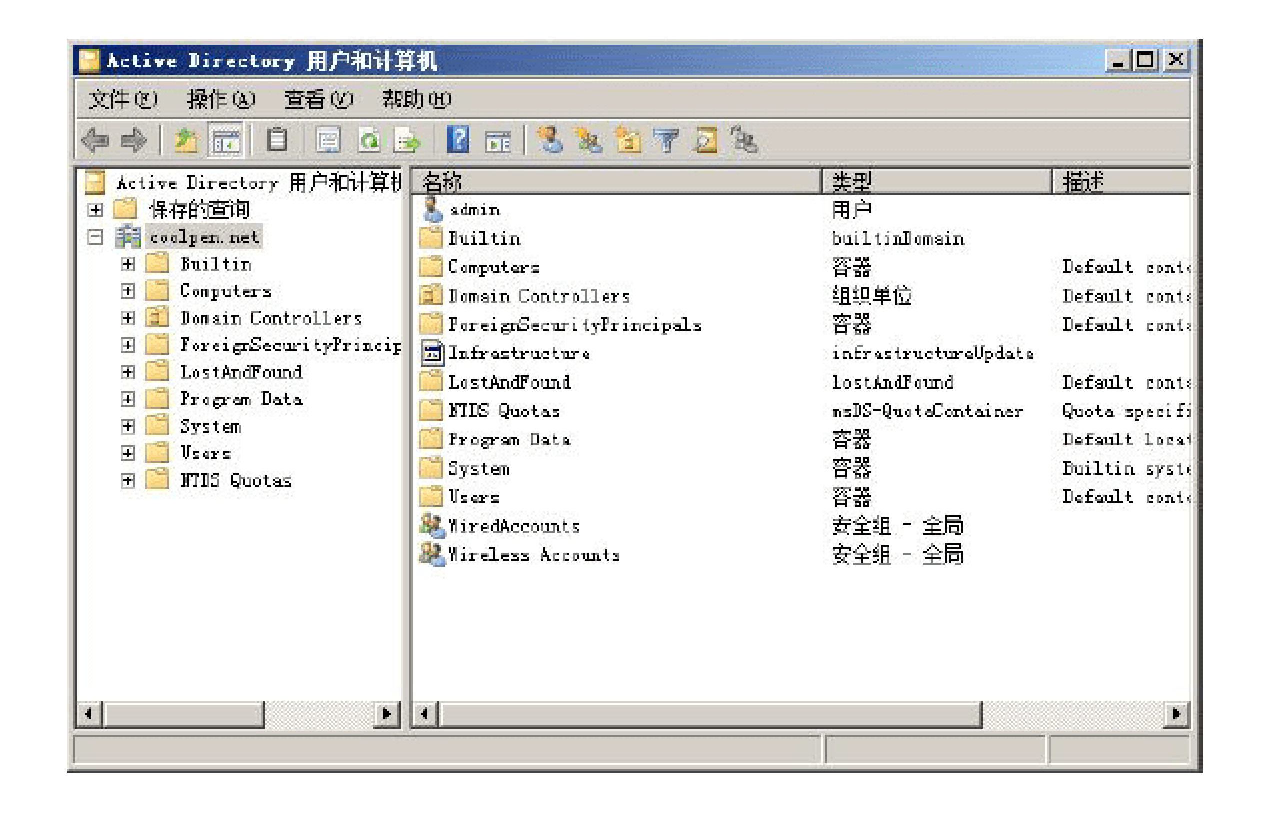


图 12-14　活动目录用户和计算机窗口

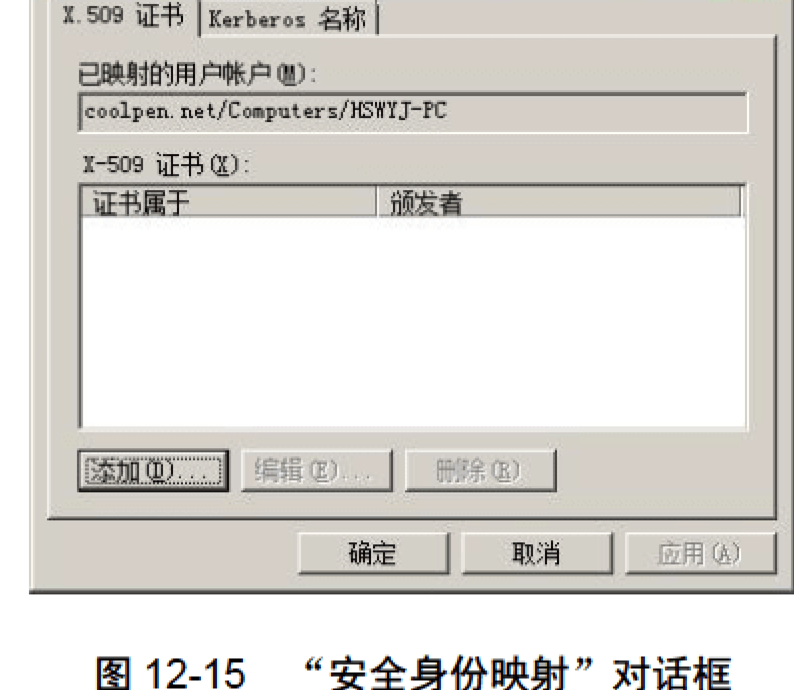


图 12-15　“安全身份映射”对话框

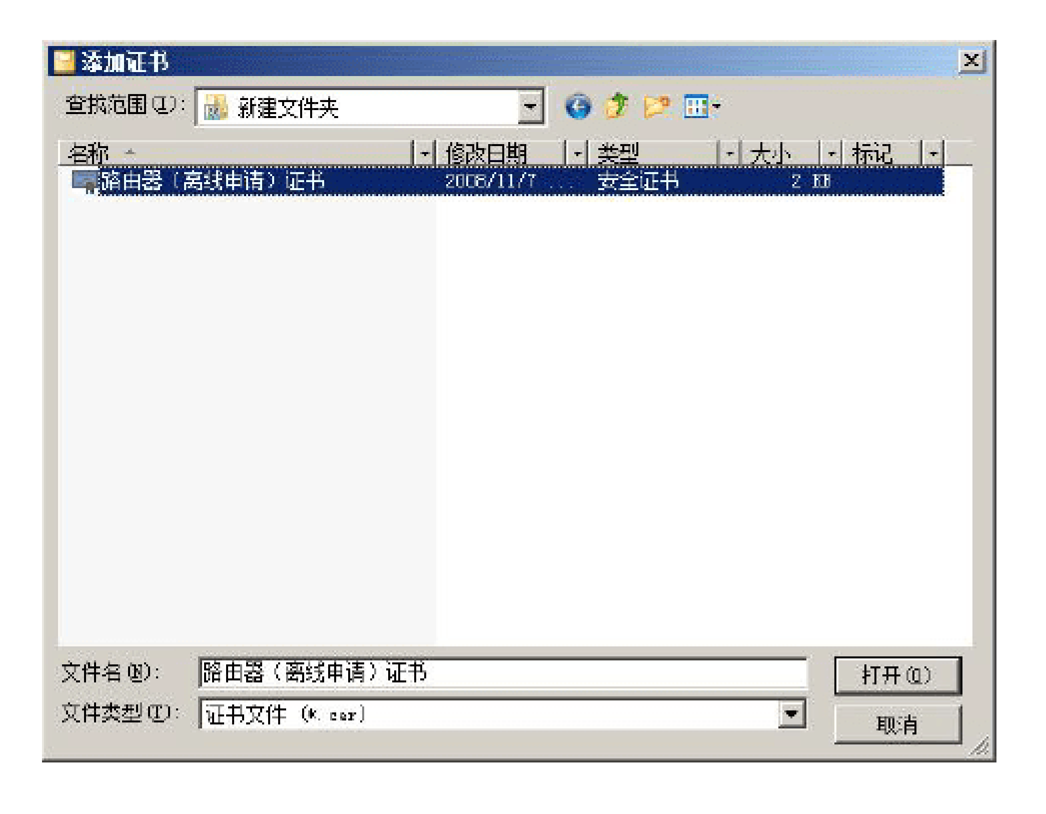


图 12-16　选择.cer 证书文件

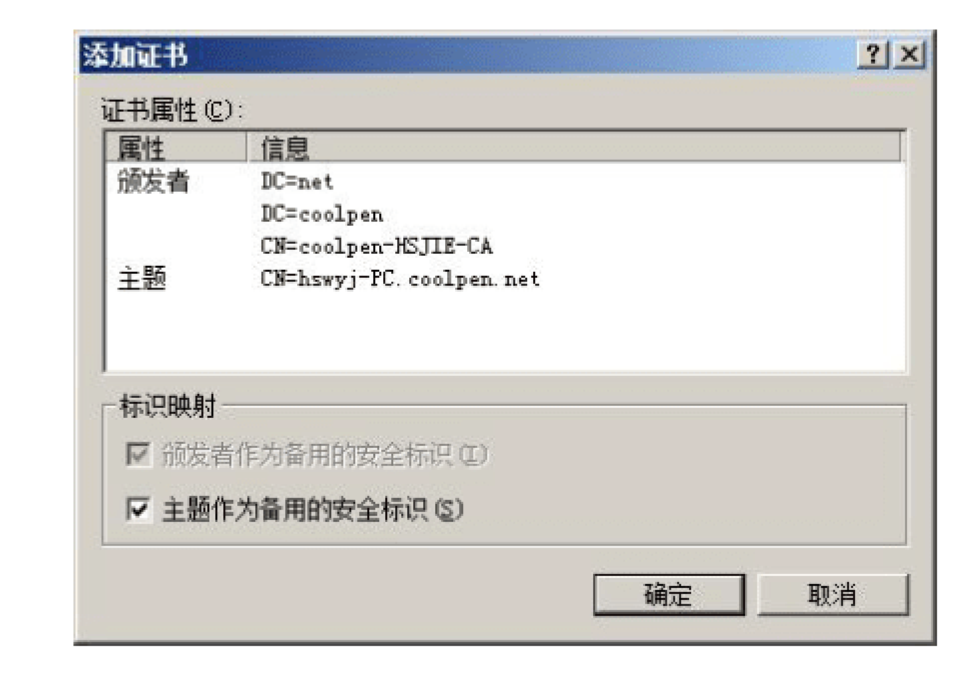


图 12-17　“证书属性”界面

⑤　单击“确定”按钮，显示如图 12-18 所示的“安全身份映射”对话框。可以看到证书已添加到“X.509 证书”列表中。

6. 导出路由器(离线申请)证书为.PFX 文件

.PFX 格式的证书文件主要用于呼叫路由器端，导出过程中已经对文件内容加密，传输更加安全。导出过程与导出.cer 证书文件类似，下面主要介绍不同步骤。

①　在本地计算机证书控制台窗口中，右击路由器(离线申请)证书，依次选择“所有任务”→“导出”命令，单击“下一步”按钮，在如图 12-19 所示的“证书导出向导”对话框中，选择“是，导出私钥”单选按钮。

②　单击“下一步”按钮，显示如图 12-20 所示的“导出文件格式”界面，选择“个人信息交换-PKCS #12(.PFX)”单选按钮。选中“如果可能，则数据包括证书路径中的所有证书”复选框。

③　单击“下一步”按钮，显示如图 12-21 所示的“密码”界面，在“密码”和“输入并确认密码”文本框中，输入证书的私钥。

④　单击“下一步”按钮，显示“要导出的文件”对话框，输入证书文件的保存路径和名称即可。接下来的操作与导出.cer 文件完全相同，此处不复赘述。



图 12-18　“安全身份映射”对话框

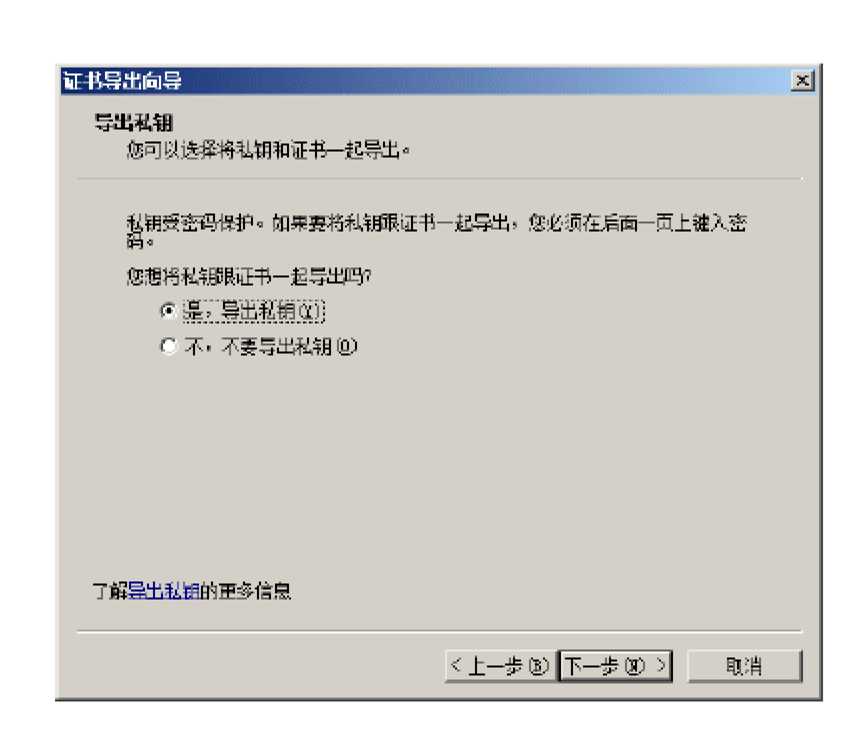


图 12-19　“证书导出向导”对话框

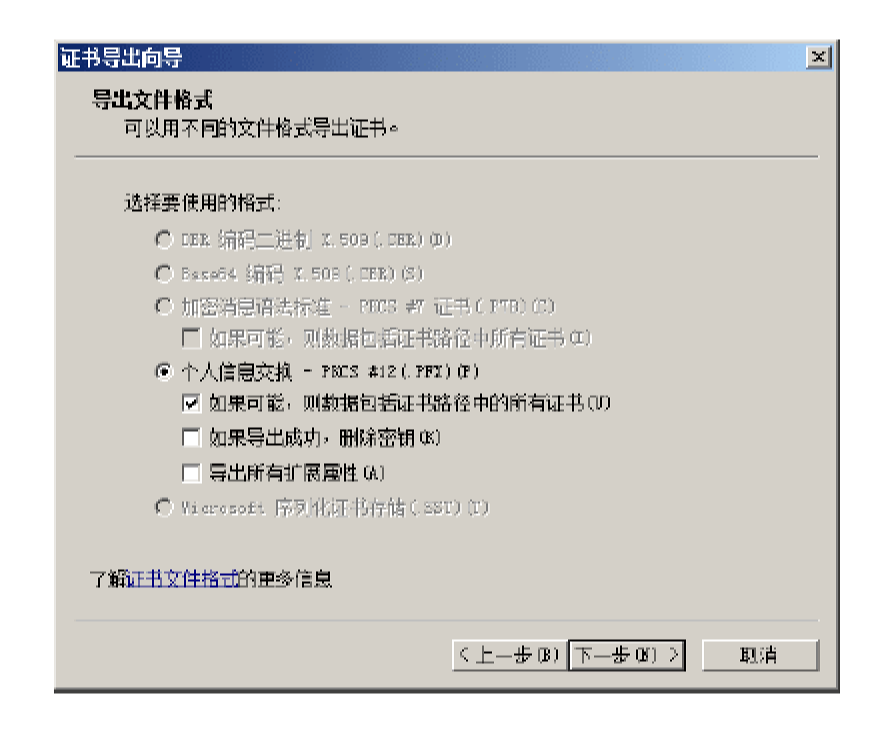


图 12-20　“导出文件格式”界面

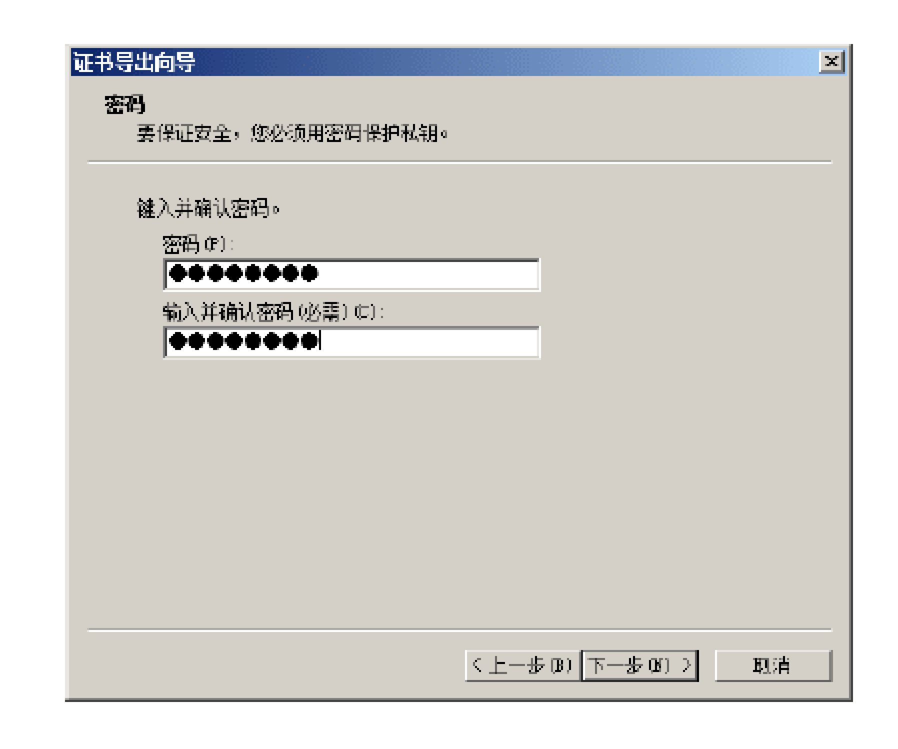


图 12-21　“密码”界面

7. 在呼叫路由器上导入路由器(离线申请).PFX 证书文件

使用可移动存储设备或者网络，将从应答路由器上导出的 PFX 证书文件发送到呼叫路由器上，接着执行如下导入过程。

① 右击证书文件并从弹出的快捷菜单中选择“安装证书”命令，显示如图 12-22 所示的“欢迎使用证书导入向导”界面。

② 单击“下一步”按钮，显示如图 12-23 所示的“证书存储”界面。选择“将所有的证书放入下列存储”单选按钮，然后单击“浏览”按钮，选择“个人”选项。



图 12-22　“欢迎使用证书导入向导”界面

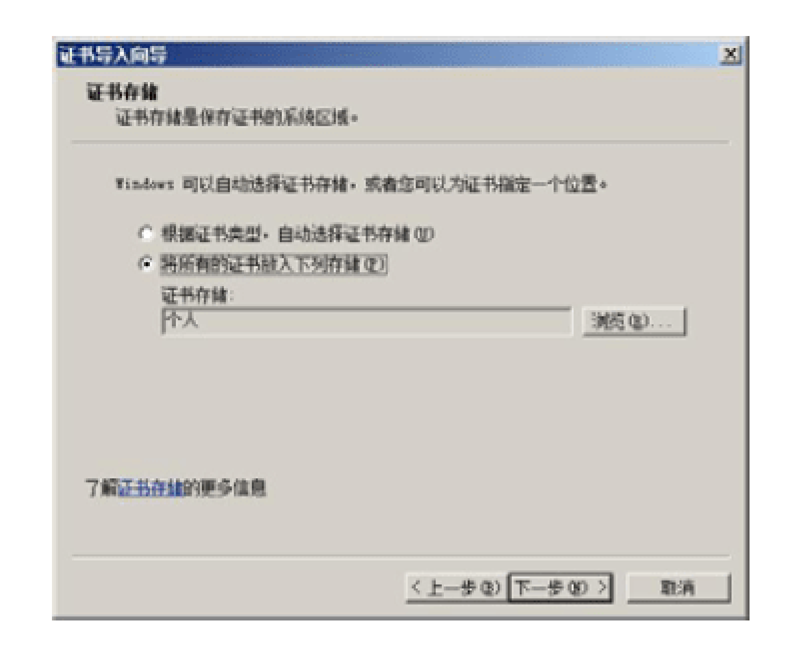


图 12-23　“证书存储”界面

③ 单击“下一步”按钮，显示如图 12-24 所示的“正在完成证书导入向导”界面。

④ 单击“完成”按钮，弹出如图 12-25 所示的“导入成功”提示框。

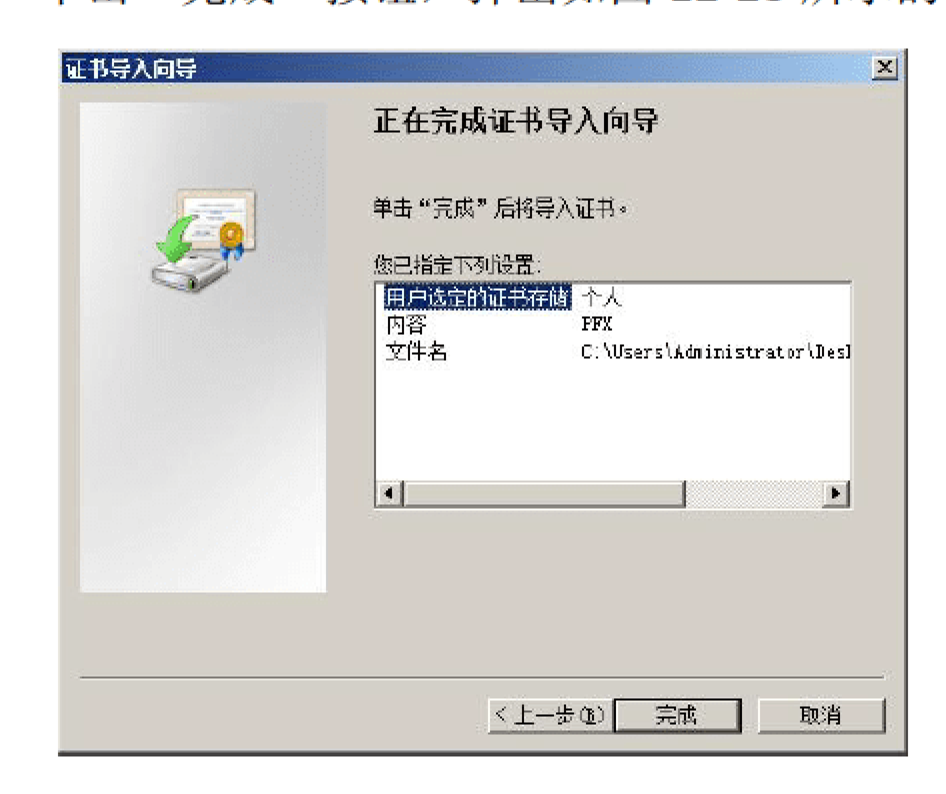


图 12-24 “正在完成证书导入向导”界面



图 12-25 “导入成功”提示框

12.3.2 配置拨入用户账户

如果用户在请求拨号接口向导中配置自动呼叫路由器添加用户账户，那么将自动配置正确的用户账户设置。如果用户手动创建呼叫路由器的用户账户，应确保在“拨入”选项卡中，网络访问权限必须设置为“允许访问”或者“通过 NPS 网络策略控制访问”，如图 12-26 所示。

另外，在“账户”选项卡中，必须确保已经取消选中“用户下次登录时须更改密码”复选框，并且选中“密码永不过期”选项框，如图 12-27 所示。



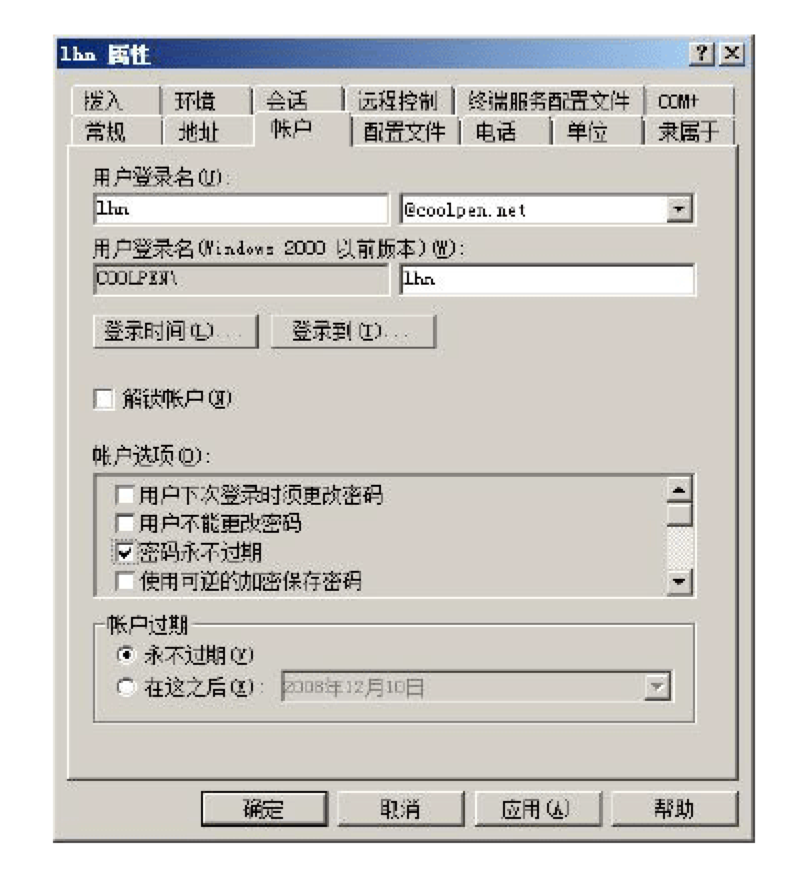


图 12-26 “拨入”选项卡

图 12-27 “账户”选项卡

12.3.3 配置 RADIUS 服务器

在点对点 VPN 连接中，RADIUS 服务器主要负责验证拨入用户账户的身份，以及对访问和操作过程进行记账。RADIUS 服务器上相关策略的配置，与远程访问 VPN 连接完全相同。详细操作可参考第 11 章中的

相关内容。

12.3.4 配置应答路由器

1. 准备工作

配置站点对站点 VPN 连接的应答路由器之前，应确保已经完成如下准备工作：

- 如果使用 L2TP/IPSec 或 EAP-TLS 方式建立安全连接，必须先在应答路由器上安装计算机证书。
- 为应答路由器配置正确的 IP 地址、DNS 服务器和内网 WINS 服务器。为了防止默认路由与指向 Internet 的默认路由冲突，用户不要在内网连接中配置默认网关。
- 运行“路由和远程访问”服务器安装向导，安装和配置 VPN 服务器。
- 配置请求拨号接口。

2. 安装和配置应答路由器

与安装远程访问 VPN 连接相同，用户需要先运行“路由和远程访问”服务器安装向导，安装 VPN 服务器。具体安装过程可参考本书第 11 章中的相关内容，此处不复赘述。默认情况下，“路由和远程访问”服务器安装向导，不会自动启用本地 IPv6 功能。在点对点的 VPN 连接中，用户还可以根据需要启用站点内网的 IPv6 功能。

① 打开“路由和远程访问”窗口，右击 VPN 服务器的名称，在弹出的快捷菜单中选择“属性”命令，显示如图 12-28 所示的服务器属性对话框。选中“IPv6 路由器”复选框，选择“局域网和请求拨号路由”单选按钮。

② 切换至如图 12-29 所示的 IPv6 选项卡，选中“启用 IPv6 转发”和“启用默认的路由通告”复选框。输入分配给基于 IPv6 的 VPN 路由器的子网前缀，用户不需要指定前缀长度。




图 12-28 服务器属性对话框



图 12-29 IPv6 选项卡

③ 单击“确定”按钮，弹出如图 12-30 所示的“路由和远程访问”提示框。单击“是”按钮即可。

3. 配置请求拨号接口

① 打开“路由和远程访问”窗口，右击“网络接口”，在弹出的快捷菜单中选择“新建请求拨号接口”命令，显示如图 12-31 所示的“欢迎使用请求拨号接口向导”界面。

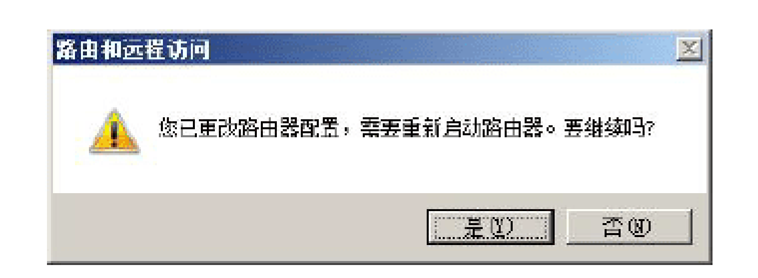


图 12-30 “路由和远程访问”提示框



图 12-31 “欢迎使用请求拨号接口向导”界面

② 单击“下一步”按钮，显示如图 12-32 所示的“接口名称”界面，输入请求拨号接口的名称。对于双向连接，该名称与呼叫路由器的用户证书的用户名称相同。

③ 单击“下一步”按钮，显示如图 12-33 所示的“连接类型”界面，选择“使用虚拟专用网络(VPN)连接”单选按钮。



图 12-32 “接口名称”界面



图 12-33 “连接类型”界面

④ 单击“下一步”按钮，显示如图 12-34 所示的“VPN 类型”界面，根据需要选择“自动选择”、“点对点隧道协议(PPTP)”或“第 2 层隧道协议(L2TP)”单选按钮。

⑤ 单击“下一步”按钮，显示如图 12-35 所示的“目标地址”界面，输入呼叫路由器的名称、IPv4 地址或 IPv6 地址。对于单向的站点对站点 VPN 连接，用户可以跳过这一步。

⑥ 单击“下一步”按钮，显示如图 12-36 所示的“协议及安全”界面。如果已经通过其他方式为呼叫路由器创建了用户账户，则此处使用默认设置即可；否则，可以选中“添加一个用户账户使远程路由器可以拨入”复选框，同时创建相关用户账户。

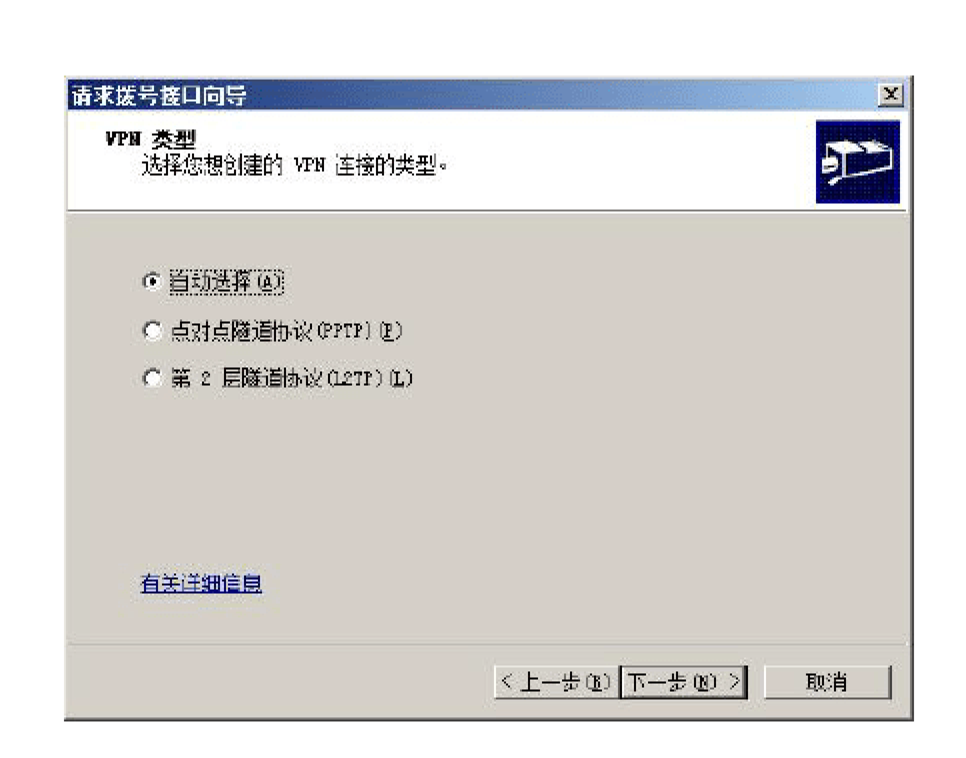


图 12-34 “VPN 类型”界面

⑦ 单击“下一步”按钮，显示“远程网络的静态路由”界面。单击“添加”按钮，显示如图 12-37 所示的“静态路由”对话框，来添加分配给请求拨号接口的静态路由。添加能够概括呼叫路由器

站点的 IPv4 和 IPv6 地址空间的静态路由，单击“确定”按钮。

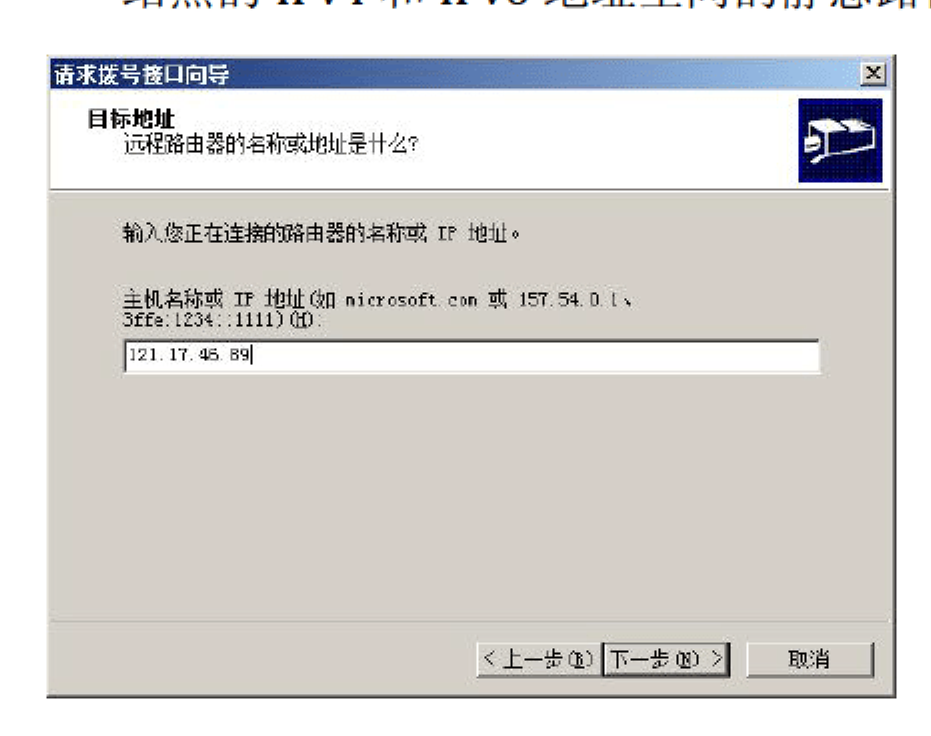


图 12-35　“目标地址”界面



图 12-36　“协议及安全”界面

⑧ 单击“下一步”按钮，显示如图 12-38 所示的“拨入凭据”界面。在“密码”和“确认密码”文本框中，输入呼叫路由器的用户账户的密码。

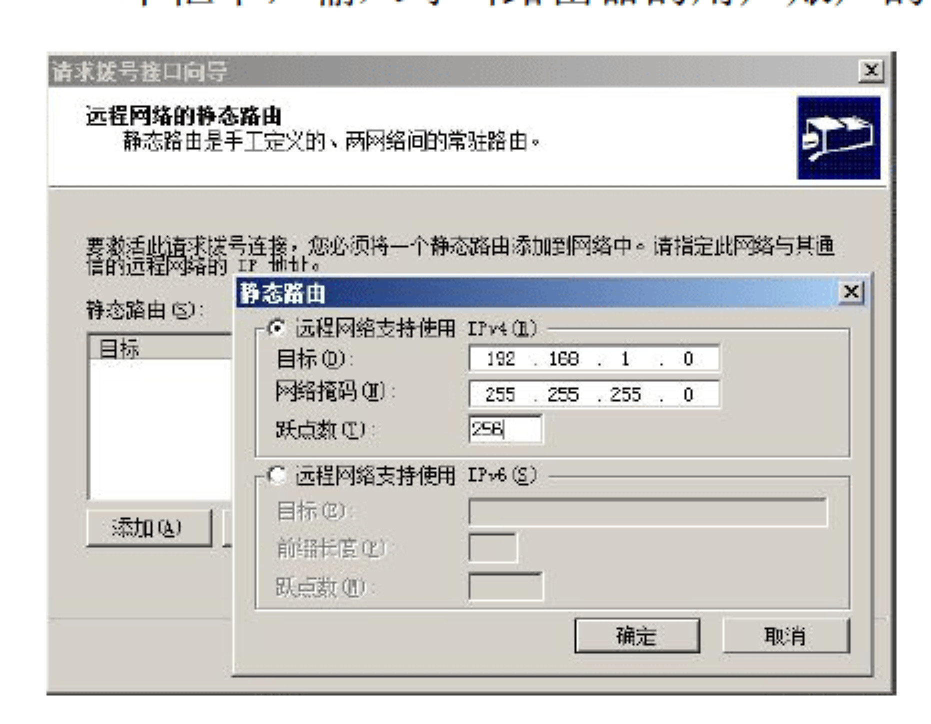


图 12-37　“静态路由”对话框

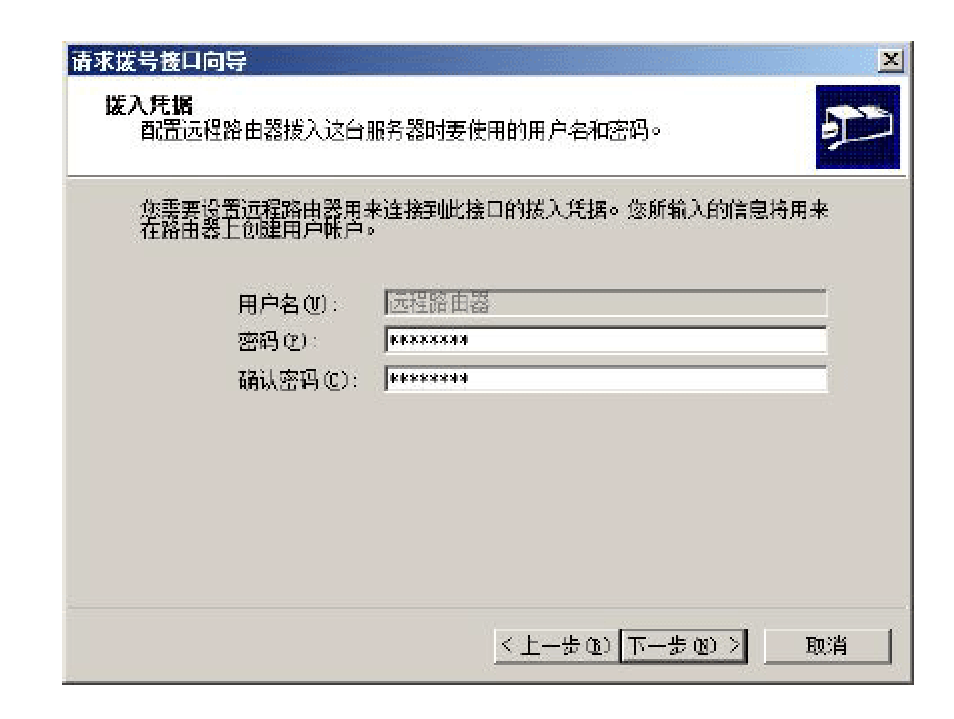


图 12-38　“拨入凭据”界面

⑨ 单击“下一步”按钮，显示如图 12-39 所示的“拨出凭据”界面。在“用户名”文本框中输入用户名，在“域”文本框中输入账户域名称，并且在“密码”和“确认密码”文本框中输入账户密码。

⑩ 单击“下一步”按钮，显示如图 12-40 所示的“完成请求拨号接口向导”界面，单击“完成”按钮。



图 12-39　“拨出凭据”界面



图 12-40　“完成请求拨号接口向导”界面

12.3.5 配置呼叫路由器

在双向初始化连接的站点对站点 VPN 连接中，呼叫路由器的配置与应答路由器的配置完全相同。但是在配置请求拨号接口时，应注意选择与应答路由器端完全相同的 VPN 类型。推荐两端均设置为“自动选择”，如图 12-41 所示。详细配置过程，可参考配置应答路由器的相关内容，此处不复赘述。

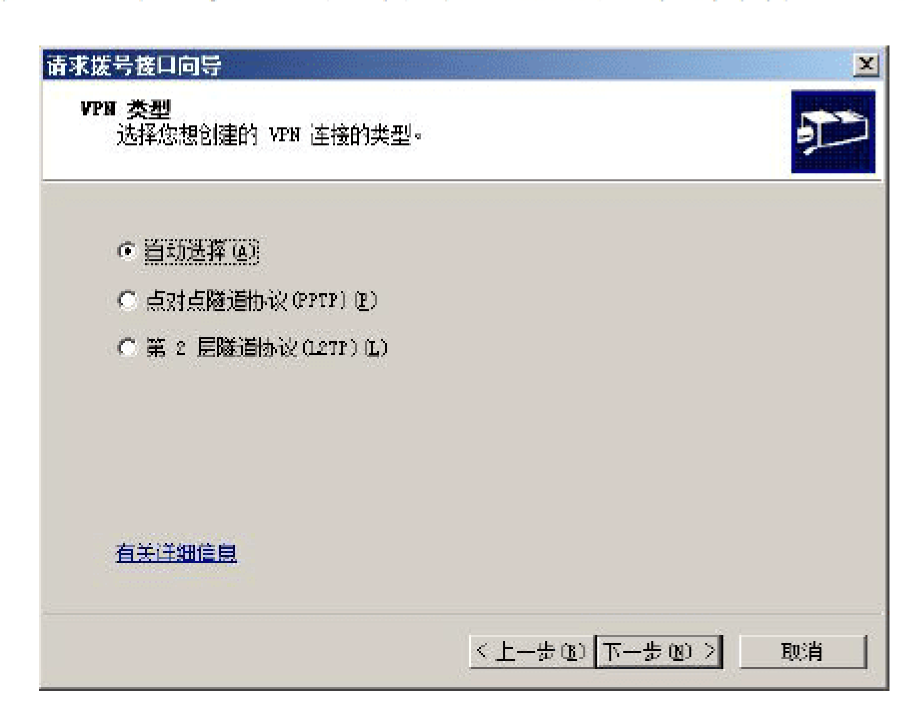


图 12-41　选择 VPN 类型

12.3.6 配置站点网络基础结构

为确保站点服务器能够正确转发对端网络到本地网络的访问，必须在每台 VPN 路由器上做好如下配置：

- 配置 VPN 路由器上的路由。
- 验证每台 VPN 路由器的可到达性。
- 配置 Off-subnet 地址池的路由(可选)。
- 为 VPN 路由器配置 IPv6 子网前缀的路由。

1. 配置 VPN 路由器的路由

为了使 VPN 路由器能够在站点中正确转发通讯，用户必须添加概括站点中所使用的 IPv4 和 IPv6 地址空间的静态路由。对于 IPv4，用户可以使用 RIP IPv4 路由连接 VPN 服务器，保证 VPN 路由器可以与临近的 RIP 路由器交换路由，并且为站点子网自动添加路由到路由表中。详细配置过程，可参考第 11 章中的相关内容。

2. 验证每台 VPN 路由器的可到达性

使用 Ping 命令、Windows Internet 浏览器和建立驱动打印机连接来验证 VPN 路由器是否可以成功与内网资源进行通信。

3. 配置 Off-subnet 地址池的路由

如果用户使用 IPv4 地址池配置 VPN 路由器，而且每个池都是 Off-subnet，那么必须确保对应 Off-subnet 地址池的路由存在于内网 IPv4 路由基础结构中。用户可以添加对应 Off-subnet 地址池的静态路由到 VPN 路由器的临近路由器中，然后通过内网路由协议将路由传播到其他路由器中。当用户添加静态路由时，必须指定网关或下一跳的地址是 VPN 路由器的内网接口。

4. 为 VPN 路由器配置 IPv6 子网前缀的路由

为了确保 IPv6 VPN 路由器从内网可到达，用户必须为呼叫路由器添加对应子网前缀的静态路由到应答路由器临近的 IPv6 路由器中，然后通过内网路由协议传播路由到其他路由器上。当用户添加静态路由时，必须指定网关或下一跳地址为 VPN 路由器的内网接口链接——本地地址。

12.3.7　配置站间网络基础结构

站间网络基础结构主要是指使用 IP 地址空间的路由，设置配置每台 VPN 路由器。在请求拨号接口向导中，在“远程网络静态路由”界面，用户可以添加静态 IPv4 或 IPv6 路由到请求拨号接口。这些路由包含了其他 VPN 路由器站点的 IPv4 和 IPv6 地址空间。如果需要添加更多路由，用户必须完成如下工作：

- 在每台 VPN 路由器上手动配置静态路由。
- 在每台 VPN 路由器上执行自动静态更新。
- 配置站点对站点 VPN 连接的路由协议操作。

1. 在每台 VPN 路由器上手动配置静态路由

用户可以手动配置其他 IPv4 或 IPv6 静态路由。以 IPv4 静态路由为例，在“路由和远程访问”窗口中，展开“IPv4”，右击“静态路由”，在弹出的快捷菜单中选择“新建静态路由”命令，显示如图 12-42 所示的“IPv4 静态路由”对话框。选择请求拨号接口，然后输入静态路由的目标、网络掩码和跃点数。用户也可以选中“使用此路由来初始化请求拨号连接”复选框，建立匹配该路由的请求拨号连接。最后单击“确定”按钮，保存配置。


提示：重复上述操作可以添加多条静态路由。IPv6 静态路由的设置与之完全相同，此处不复赘述。

2. 在每台 VPN 路由器上执行自动静态更新

如果在 VPN 路由器的请求拨号接口启用了 IPv4 RIP 路由协议，则当 VPN 连接处于连接状态时，用户可以使用自动静态更新来自动配置 IPv4 静态路由。在“路由和远程访问”窗口，依次展开“IPv4”→“常规”节点，检查请求拨号接口的可选状态区，确保其处于连接状态。右击请求拨号接口并从弹出的快捷菜单中选择“更新路由”命令即可，如图 12-43 所示。

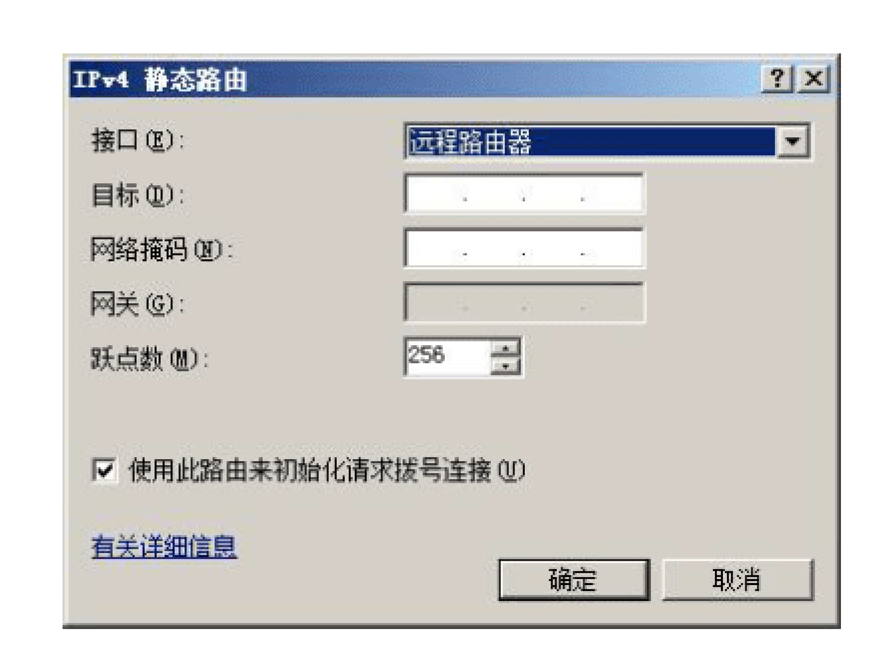


图 12-42　“IPv4 静态路由”对话框

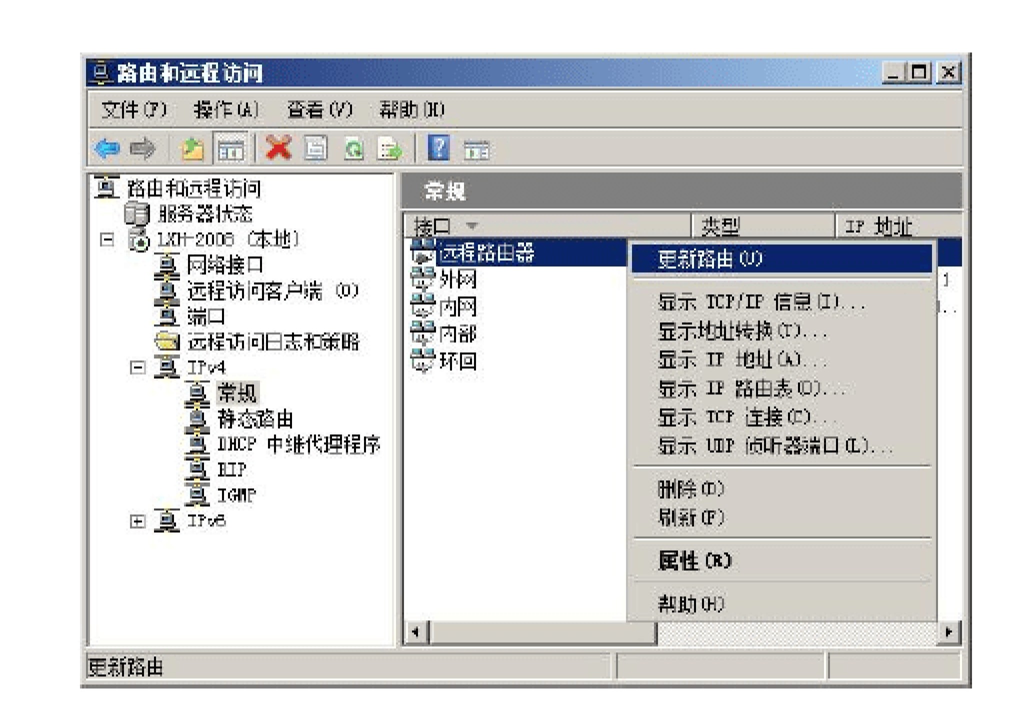


图 12-43　自动静态更新路由

用户也可以运行命令 Netsh 来执行自动静态更新，或者通过混合使用 Netsh 脚本和任务调度器来自动执行更新。为了使用 RIP 为特定请求拨号接口自动执行静态更新，运行如下命令：

```
netsh interface set interface name=DemandDialInterfaceName connect=CONNECTED
netsh routing ip rip update name=DemandDialInterfaceName
netsh interface set interface name=DemandDialInterfaceName connect=DISCONNECTED
```

例如，为了使用名为 CorpHub 的请求拨号连接自动更新 IP 路由，输入如下命令：

```
netsh interface set interface name=CorpHub connect=CONNECTED
netsh routing ip rip update name=CorpHub
netsh interface set interface name=CorpHub connect=DISCONNECTED
```

用户可以从一批文件中运行这些命令，或者将它们放置在 Netsh 脚本文件中。例如，在脚本文件 CorpHub.scp 中包含运行如下命令：

```
interface set interface name=CorpHub connect=CONNECTED
routing ip rip update name=CorpHub
interface set interface name=CorpHub connect=DISCONNECTED
```

为了运行 CorpHub.scp 脚本文件，输入如下命令：

```
Netsh -f corphub.scp
```

在创建完分批文件或 Netsh 脚本文件后，用户可以通过任务调度器执行这些文件。

3. 配置路由协议

如果站点对站点 VPN 连接是持续的，则用户可以在 VPN 路由器的请求拨号接口上配置 IPv4 的 RIP 路由协议，自动更新每个 VPN 路由器的 IPv4 路由。

第 13 章　网络访问保护概述

NAP 英文全称为 Network Access Protection(网络访问保护)。在 Windows Server 2008、Windows Vista 和 Windows XP SP3 中，提供了新型的 NAP 平台和 NAP 组件，可以使用不同类型的 NAP 强制方法工作。例如 IPSec 强制、VPN 强制等。

关键词

- 网络访问保护的需要
- NAP 的组件
- 强制方式
- NAP 工作方式
- 网络访问保护的准备

13.1 网络访问保护的需要

为了理解 NAP 的必要性，首先需要了解一些阻止恶意软件传播的方法，例如恶意软件的威胁和传播方法、恶意软件防护技术，以及 NAP 如何提供集中式的定义、整合和系统健康所需要的强制，帮助专有网络防止恶意软件等。

13.1.1 恶意软件及其对企业计算机的影响

目前，在计算机网络中充满了恶意攻击者的影子。很多恶意软件使用与 E-mail、文件传输、Web 访问和实时合作等相同的计算机网络技术，并利用这些网络应用本身的弱点进行攻击。通常情况下，恶意软件会安装在不具备防护、数据访问知识用户的计算机上，用来报告计算机的活动，或使用其他计算机对其进行控制。目前流行的恶意软件包括计算机病毒、间谍软件和广告软件等。

Internet 是一个特别容易受到攻击的环境，一台安全性不高的计算机可能会在几分钟之内被地址和端口扫描软件入侵。家庭网络同样也是一个危险的环境，因为家庭计算机不仅会被地址扫描和端口扫描恶意软件攻击，而且通过 E-mail 附件、Web 控制和免费软件中的特洛伊木马传播的恶意软件也会对家庭计算机进行攻击。而处于局域网内的计算机，则因为不是直接连接到 Internet 上，相对比较安全。但也只是相对意义上的安全，在局域网内的计算机同样会受到病毒等安全问题的影响，并且一旦受到攻击，其损害程度比家庭计算机更为严重。

1. 恶意软件如何进入企业网络

通常企业网络环境都不是直接连接到 Internet 上的，只有部分计算机直接连接到 Internet，为客户或商业伙伴提供 Internet 服务。大部分的计算机和 Internet 之间被防火墙和代理服务器等边界系统隔离。所以，企业网络中的计算机通常不会被来自 Internet 的病毒扫描攻击。

但是，对防火墙或代理服务器提供的边界安全，会面对如下问题：

- 通过在计算机上执行基于特洛伊木马的病毒。企业网络中的用户可能在不经意间就从 E-mail、Web 页面或 Internet 上下载的其他类型的文件中感染了病毒。其中，E-mail 附件是传播特洛伊木马病毒最常见的方式，Web 页面是另外一种常见的方式。
- 移动和连接其他网络的移动计算机。移动计算机的典型代表是便携式计算机，即通常所说的笔记本电脑。用户将便携式计算机带到家里、商业旅途中或其他具有无线热点的公共场所中。每次用户都可以将便携式计算机连接到非企业网络上，此时，便携式计算机都可能受到网络级病毒的攻击。
- 职员远程访问。当职员使用远程访问连接企业网络时，理论上如同在职员所在地到企业网络端口之间有以太网线路一样。通过逻辑连接，企业网络可能会受到网络级病毒的攻击。
- 来宾计算机。当企业的来宾(如顾问、提供商或商业伙伴)使用计算机连接企业网络时，他们所使用的计算机之前可能已经受到网络级病毒的攻击。

2. 恶意软件的影响

对于 Internet 和专有网络来说，恶意软件可能会带来直接的经济影响。例如，机密信息的泄露、知识产权的丢失、带宽的浪费、计算机行为的不可用，以及为了从所有感染的计算机上移除恶意软件所花费的

时间等。

13.1.2　在企业网络中防止恶意软件

为了防止基于恶意软件的传播，IT 企业开始防止未来病毒的感染，从而出现了一系列的恶意软件防护技术，以及从事该工作的很多企业和用户。

1. 恶意软件防护技术

恶意软件防护程序是用来防止恶意软件安装和传播的。恶意软件防护程序具有如下形式。

- 杀毒软件：在文件复制或下载时监视已知的恶意软件。杀毒软件通常使用本地病毒库来识别 E-mail 和文件中的恶意软件。如果恶意软件被检测到，杀毒软件将会移除恶意软件或者阻止文件被存储或执行。因为会不停地有新型的病毒被创建，所以杀毒软件的病毒库需要定期更新。
- 垃圾邮件过滤：用来阻止不需要的 E-mail 消息存储到 E-mail 邮箱的软件。垃圾邮件是传播病毒或间谍软件常用的方式。
- 反间谍软件：从计算机上检测和移除已知间谍软件和广告软件的软件。如同杀毒软件一样，反间谍软件必须定期更新，使其可以阻止最新的间谍软件的安装。例如，Windows Vista 中的 Windows Defender 就是一款反间谍软件。

除了恶意软件防护软件之外，采用下列技术也可以防止恶意软件。

- Windows 计算机的自动更新：对于运行 Windows 的计算机，一些类型的病毒会针对系统安全隐患进行攻击，所以安全更新是很有必要的。病毒会尝试攻击没有进行更新的计算机。为了在病毒编写者写出恶意软件并传播之前进行自动安全更新，微软会在发现漏洞的第一时间开发并发布补丁程序，供用户下载和安装。根据用户制定的计划，运行 Windows Vista、Windows Server 2008、Windows XP 或 Windows Server 2003 的计算机，可以获取 Windows 更新 Web 页面和下载最新的安全更新，并自动进行安装。Windows 更新降低了 IT 管理者为了保持计算机更新始终最新的负担。
- 基于主机的全状态防火墙：基于主机的全状态防火墙运行在计算机上，监视网络通信的数据包，阻止计算机发送或接收恶意通信。一些病毒会通过扫描本地子网可用计算机来尝试自动复制，然后攻击找到的计算机。如果成功，那么病毒将会从一台计算机复制到另外一台。如果一台受感染的计算机迁移，那么病毒就开始攻击新的子网中的计算机。例如，当便携式计算机在家庭网络受到感染，病毒将会被携带到企业的专有网络。基于主机的全状态防火墙，如 Windows Vista、Windows Server 2008、Windows XP SP2 和 Windows Server 2003 SP1 或 SP2，将会丢弃所有不符合计算机请求回复的入站通信，或被允许的主动提供的通信。例如，符合用户或计算机的 Web 页面请求的通信就是请求入站通信。由于计算机运行服务器服务而被允许，并且必须接收主动提供的请求，就是例外通信的例子。因为通常的基于网络的病毒依靠主动提供的入站通信来进行传播和攻击计算机，启用连接到 Internet 和内网的计算机上的基于主机的全状态防火墙，可以阻止这种类型病毒的传播。

为了防止恶意软件进入和蔓延到企业网络中，管理员需要确保如下工作：

- 确保用户主机计算机正在使用当前权限级别的网络服务和用户账户。通过降低用户的权限级别，可以有效地阻止恶意软件安装在主机计算机上。例如，运行 Windows Vista 的计算机使用用户账户控制(UAC)来降低被攻击的危险性。

- 使用恶意软件防护软件，定期进行更新。
- 启用自动更新，当 Windows 升级包可用时立即安装。企业网络也可以通过中央服务器(如 Windows 服务器更新服务)来配置更新服务。
- 使用基于主机的全状态防火墙，如 Windows 防火墙，来阻止网络级病毒的入侵。

2. 计算机系统健康和监视

恶意软件防护技术的使用为 IT 管理员带来了新的问题，即确定和监视内网中的计算机系统健康。该系统健康由计算机当前的配置状态定义，包括一系列的恶意软件防护技术，及其当前状态和其他配置设置。

(1) 确定系统健康要求

系统健康的定义会根据企业安装的恶意软件防护技术、计算机配置和其他安全需求而改变。为了设置系统健康需要的参数，管理员需要注意如下问题：

- 杀毒软件
  - 在整个企业网络的所有计算机上均安装防毒程序。
  - 当前计算机的防毒签名文件或其他更新需要考虑健康问题。
- 垃圾邮件过滤软件
  - 在整个企业网络中安装垃圾邮件过滤软件。
  - 当前计算机的垃圾邮件过滤更新需要考虑健康问题。
- 反间谍软件
  - 在整个企业网络安装反间谍软件。
  - 当前计算机的反间谍更新需要考虑健康问题。
- 操作系统自动更新
  - 在整个企业网络启动 Windows 自动更新。
  - 对于考虑健康的计算机启用自动更新。
  - 当前计算机安装的更新需要考虑健康问题。
- 基于主机的全状态防火墙
  - 在整个企业网络启用基于主机的全状态防火墙。
  - 对于考虑健康的计算机必须启用防火墙的问题，以及需要配置的例外。
- 其他配置设置
  - 根据企业安全策略需要其他配置设置。
  - 对于考虑健康的计算机需要的设置。

例如，管理员可以创建系统健康策略，要求所有计算机必须满足如下条件。

- 所有操作系统更新必须在指定日期进行安装。
- 必须安装杀毒软件，并运行其监视入站和出站文件。
- 杀毒软件必须安装最新版本的病毒库。
- 必须安装垃圾邮件过滤软件，并用其监视入站的 E-mail 消息。
- 垃圾邮件过滤软件必须安装最新的更新。
- 安装并启用基于主机的全状态防火墙。
- 基于主机的防火墙必须拥有一个授权的排除列表。
- 计算机上的 TCP/IP 协议栈必须禁用 IP 路由。
- 计算机上的 TCP/IP 协议栈必须启用自动获得 IP 地址。

需要注意的是，管理员面对的最大问题不是为系统健康设置要求，而是保证企业网络中的所有计算机满足这些要求，以及对不满足要求的计算机执行强制机制。

(2) 强制系统健康要求

确定系统健康是否满足企业网络中计算机的强制系统健康要求。换句话说，如果企业网络中的计算机不满足系统健康的要求，就会存在问题。例如，可以设置不符合系统健康要求的计算机禁止与网络中的其他计算机进行通信。

尽管大部分的恶意软件防护软件都拥有自己的保持更新的机制，但却没有系统健康要求的强制机制。例如，如果杀毒程序没有进行最近的更新，那么对于计算机和计算机用户来说就没有保障。

为了确保系统健康可强制，在局域网中必须拥有一台中央计算机来评价系统健康，并且对其使用企业的系统健康要求进行配置。网络中尝试连接通信的客户端计算机必须拥有自己的健康评估，以便可以检测到不符合的计算机。中央系统健康评估计算机必须对不符合的计算机采取措施。对于不符合的计算机采取的常见措施是拒绝其连接网络。但是，这种极端的措施不会为不符合的计算机提供更正其配置状态的机会。

与阻止所有内网的访问相比，更好的允许不符合的计算机更正状态的解决方案，是允许对包含所需更新、软件、脚本或其他资源的内网服务器的子网进行受限访问。例如，在受限访问逻辑网络上的服务器包括杀毒或软件更新服务器。通过使用评估系统健康的中央计算机上的资源和基础结构，不符合的计算机可以自动更正其配置。

13.1.3　NAP 的角色

Windows Server 2008、Windows Vista 和 Windows XP SP3 中的 NAP 提供组件和应用程序接口(API)设置，可以帮助管理员强制服从网络访问或通信的健康要求策略。使用 NAP，开发者和管理者可以为连接到网络的计算机创建解决方案，提供到健康更新资源需要的更新或访问，以及限制不符合的计算机的访问或通信。第三方提供商可以支持功能强大的 NAP 来为强制健康策略创建常用的解决方案。对于监视访问的健康策略遵从性，网络计算机管理员可以自定义运行状况维护解决方案的开发和部署，自动更新计算机的软件，以满足健康策略要求，或限制不符合健康策略要求的计算机的访问。

使用 NAP，基于 Windows 的网络基础架构可以完成如下任务：

- 管理员可以为 NAP 计算机配置系统健康需求。
- 管理员可以为启用 NAP 和未启用 NAP 的计算机指定访问强制动作，包括如下方面。
    - 监视计算机的访问和通信尝试，在服务器日志中记录访问尝试。
    - 为不符合或未启用 NAP 的计算机强制网络访问约束。
- 启用 NAP 的计算机可以自动进行更新变为符合，并且保持符合性。

1. NAP 的特性

NAP 具有如下三个主要特性。

- 健康状态验证：当计算机尝试连接网络时，验证计算机的健康状态是否与管理员指定的健康要求策略一致。如果计算机不符合，管理员也可以指定做法。在只监视的环境中，所有计算机都有其健康状态评估，符合健康要求策略的计算机可以进行无限制的访问；不符合健康要求策略的计算机，将进行受限的访问。
- 健康策略符合：管理员可以通过配置自动更新不符合的计算机来保证健康要求策略的符合性，配

置自动更新可以使用不可见软件更新或使用独立的管理软件产品，如 SCCM 2007。在只监视的环境中，计算机在更新或配置更改之前将会访问网络。在受限访问环境中，不符合的计算机在更新和配置更改完成之前只能进行受限访问。在这两种环境中，符合 NAP 的计算机可以自动变为符合的，而且管理员可以为不符合 NAP 的计算机指定例外。

- 受限访问：根据管理员指定的策略，管理员可以通过限制不符合的计算机的访问来保护网络。管理员可以创建包含健康更新资源和其他服务器的受限网络，不符合的计算机只能访问受限网络。管理员也可以配置例外，使得不符合 NAP 的计算机不受网络访问的限制。

2. 典型的 NAP 方案

NAP 为如下常见需求提供解决方案。

- 便携式计算机健康状态的验证：轻便性和机动性是便携式计算机的两个主要优势，但是这些特征也提供了健康威胁。当便携式计算机离开公司时，可能无法获取最新的软件更新或配置更改。当便携式计算机暴露在无保护的网络中时就可能感染病毒。通过使用 NAP，网络管理员可以检查网络中任何一台便携式计算机的健康状态，确定其是通过 VPN 连接公司网络还是通过物理链路连接办公室。
- 台式机健康状态的验证：尽管台式电脑通常不会离开公司网络，但是仍然存在网络威胁。为了降低网络威胁，必须使用最新的更新和软件来维护这些计算机；否则，这些计算机很有可能会通过 Web 站点、E-mail、共享文件和其他公共访问资源感染病毒。通过使用 NAP，可以自动进行健康状态的检查，来确定每台台式机是否符合健康要求策略。管理员可以检查日志文件，来确定哪一台计算机不符合健康要求策略。使用其他管理软件，管理员可以自动产生报告和自动更新不符合的计算机。当管理员更改健康要求策略时，计算机可以自动获取最新的更新。
- 访问便携式计算机健康状态的验证：企业有时必须允许咨询者、商业伙伴和来宾连接专有网络。来宾带来的便携式计算机可能不符合系统健康要求，而且可能存在健康威胁。通过使用 NAP，可以确定来访的便携式计算机不符合，并只允许其访问 Internet。管理员通常不会为来访的便携式计算机要求或提供任何更新或配置更改。
- 不受管理的家庭计算机健康状态的验证：不受管理的家庭计算机不是公司活动目录域的成员，可以通过 VPN 连接可管理的公司网络。不受管理的家庭计算机为管理员提供了额外的难度，因为他们不能对这些计算机进行物理访问。物理访问的缺乏使得强制健康要求符合(如杀毒软件的使用)变得更加困难。但是，使用 NAP，网路管理员可以随时确定使用 VPN 连接公司网络的家庭计算机的健康状态，只允许其访问受限网络直至满足系统健康要求。

3. NAP 的扩展性

NAP 是一个可扩展的平台，为添加确认及修正计算机健康状态和强制访问限制的组件提供基础结构和一系列的 API。

4. NAP 的局限性

NAP 不是为了保护网络不受恶意用户攻击而设计的，而是为了帮助管理员自动维护网络中计算机的健康而设计的，同时也维护了网络的完整性。例如，如果计算机拥有健康策略所需要的所有软件和配置，那么计算机符合并且被允许适当地访问网络。NAP 不会阻止授权用户使用符合的计算机上传恶意程序或参与其他不适当的行为。

13.1.4　NAP 的应用环境

网络内部安全已经成为网络安全的重点。用户水平参差不齐，使用习惯各不相同。例如，如果网络中有没有安装软件更新或者防病毒软件的客户端，则很可能导致整个网络遭受攻击。NAP 就可以很好地解决这一难题，通常情况下，它可以应用于如下保护环境。

1. 保护漫游计算机的健康

网络中应用笔记本移动办公的用户越来越广泛，例如，需要经常携带笔记本计算机出差的用户，笔记本计算机需要经常连接不安全的外部网络。如果没有安装更新补丁，没有更新病毒库，或者已经感染病毒，一旦连接到公司网络，就要进行安全检查。

2. 保护桌面计算机的健康

网络中相对比较固定的工作站，虽然可以受到网络防火墙的保护和安全策略限制，但是由于经常接入 Internet、连接移动设备、收发电子邮件等，也可能存在一定的安全隐患，有必要接受补丁包获得更新，并更新病毒库。

3. 保护来访用户计算机的健康

有时候来访用户的计算机需要连接到内部网络，但是，很难保证这些计算机符合网络内部的安全策略，如果强行接入网络，则可能存在安全威胁。此时，可以通过网络访问保护功能在技术层面进行访问限制。当客户计算机连入内部网络之后，NAP 可以将客户计算机重定向到一个隔离的网段，会自动连接到修正服务器，对客户计算机实施制定的安全策略，例如进行自动更新、修复漏洞等。在修复安全之后，客户计算机可以自动连接到内部网络。以上操作自动完成，不耽误业务的进展。

4. 保护家庭计算机的健康

网络中的用户有时候会将工作带到家中处理，需要通过 VPN 等方式将家中的计算机连接到公司内部网络访问资源，此时家中的计算机就有可能对公司内部网络造成安全威胁。使用 NAP 功能可以设置检查家庭计算机，可以将接入的家庭计算机限制到隔离网段，进行健康修复，直到安全为止。

13.1.5　NAP 的商业价值

对于企事业单位来说，NAP 具有非常高的商业价值，具体包括如下内容。

- 通过集中配置和连接或通信的系统需求降低了所有权的总花费：NAP 提供集中配置点来指定如下方面。
  - 网络中连接或通信的计算机的系统健康需求，包括恶意软件防护、软件设置或系统配置。
  - 为不满足要求的计算机强制动作。强制动作可以是被动的，允许不受限制的访问但是记录每次连接或通信尝试；或者是主动的，限制不符合的计算机的访问。



提示：在评价客户端系统设置的服务器上，系统要求和强制动作都是以健康要求策略的形式进行集中配置的。

- 通过自动系统健康或配置修正来降低所有权的总花费：启动 NAP 的计算机将会为恶意防护软件自

动安装更新，并且使必需的配置优先于授权不受限制的网络访问。尽管大部分恶意防护软件定期检查更新进行安装，但是 NAP 还要求网络连通性的更新。当启用 NAP 的计算机符合系统健康策略时，NAP 组件将会自动执行更新来保证运行符合性。

- 降低被恶意软件感染的几率：因为 NAP 平台可以强制系统健康要求，启用 NAP 的计算机可以进行更新并阻止已知的恶意软件的攻击。适当的配置启用NAP的网络可以降低恶意软件感染的几率。
- 现有系统健康和配置要求基础结构的使用：NAP 无法取代现有系统健康和配置基础结构。NAP 通过设置共同目标和强制系统健康要求，来为现有系统健康和配置组件增加价值。很多系统配置、恶意软件防护和网络安全基础结构提供商都支持 NAP。

13.2 NAP 的组件

图 13-1 显示了启用 NAP 的网络基础结构的组件。启用 NAP 的网络基础结构的组件主要包含如下内容。

- NAP 客户端：支持 NAP 的计算机包括 Windows Server 2008、Windows Vista 或 Windows XP SP3 的计算机。
- NAP 强制点：使用 NAP 或可以使用 NAP 的计算机与网络设备要求 NAP 客户端的健康状态评估，并提供受限的网络访问或通信。NAP 强制点使用网络策略服务器(NPS)作为 NAP 健康策略服务器来评估客户端的健康状态信息，网络访问或通信是否被允许，以及对不符合的 NAP 客户端必须执行的修正动作的设置。NAP 强制点的例子如下。
  - 健康注册机构(HRA)：运行 Windows Server 2008 和 Internet 信息服务(IIS)的计算机，对于符合的 NAP 客户端都具有证书颁发机构(CA)颁发的健康证书。
  - 网络访问设备：以太网交换机或支持 IEEE 802.1X 身份验证的无线访问点(AP)。
  - VPN 服务器：运行 Windows Server 2008 的计算机，以及允许远程访问 VPN 连接内网的路由和远程访问。
  - DHCP 服务器：运行 Windows Server 2008 的计算机，以及提供动态 IPv4 地址配置的 DHCP 服务器服务。
- NAP 健康策略服务器：运行 Windows Server 2008 的计算机，以及存储健康要求策略和提供健康状态验证的 NPS 服务。NPS 代替了 Internet 身份验证服务、RADIUS 服务器和 Windows Server 2003 提供的代理。NPS 也可以作为网络访问的身份验证、授权和记账(AAA)服务器。当作为 AAA 服务器或 NAP 健康策略服务器时，NPS 通常为网络访问和健康要求策略的集中配置使用单独的服务器。NPS 服务也可以运行在基于 Windows Server 2008 的 NAP 强制点上，如 HRA 或 DHCP 服务器。但在这些配置中，NPS 服务是用于 RADIUS 代理与 NAP 健康策略服务器交换 RADIUS 消息的。
- 健康要求服务器：为 NAP 健康策略服务器提供当前系统健康状态的计算机。例如，使用杀毒程序的健康要求服务器需要追踪最新版本的病毒库文件。
- 活动目录域服务：存储账户证书和属性，以及组策略设置的 Windows 目录服务。虽然不需要健康状态验证，但是活动目录需要 IPSec 保护通信、802.1X 验证连接，以及远程访问 VPN 连接。
- 受限网络：一个单独的逻辑或物理网络包含如下部分。
  - 修正服务器：网络基础结构服务器和 NAP 用来修正不符合状态的健康更新服务器。例如，网络基础结构服务器包括 DNS 服务器和活动目录域控制器。健康更新服务器包括病毒库服务器和软件更新服务器。

- 访问受限的 NAP 客户端：对于不满足健康要求策略的计算机将会被放置在受限网络中。
- 不支持 NAP 的计算机：不支持 NAP 的计算机将会被放置在受限网络中。

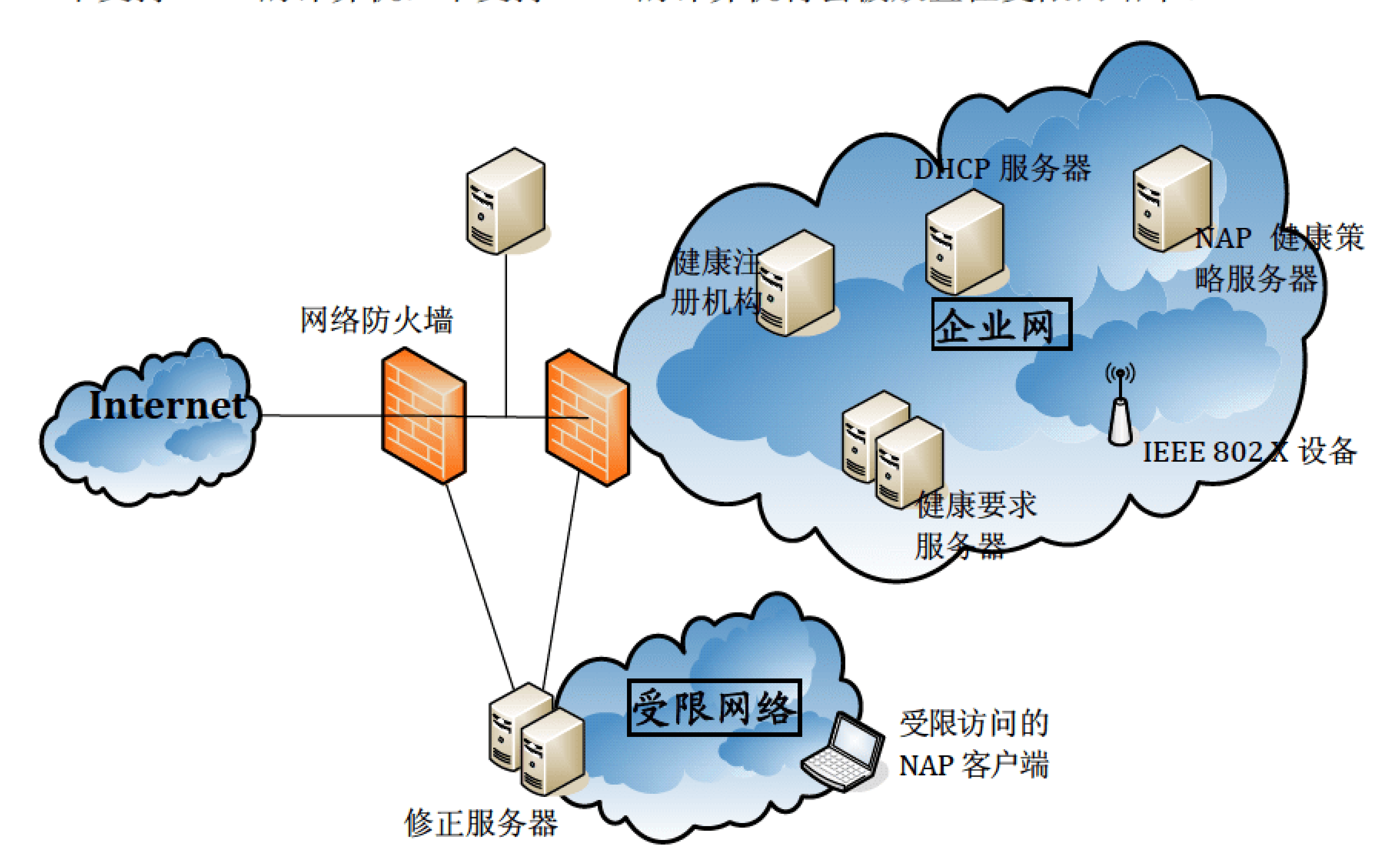


图 13-1　启用 NAP 的网络基础结构的组件

13.2.1　系统健康代理和系统健康验证

NAP 基础结构组件在 NAP 客户端中也称作系统健康代理(SHA)，在 NAP 健康策略服务器中称作系统健康验证(SHV)，为系统健康属性提供健康状态跟踪和验证。Windows Vista 和 Windows XP SP3 包含 Windows 安全健康验证 SHV，用来监视 Windows 安全中心的设置。在 Windows Server 2008 中，包含相应的 Windows 安全健康验证 SHV，NAP 具有灵活性和可扩展性。

SHA 创建一个健康声明(SoH)，其中包含当前监视的健康状态信息。例如，对于属性程序的 SHA 可能包含程序的状态(安装或运行)，以及当前反病毒签名文件的版本。只要 SHA 升级其状态，就会创建一个新的 SoH。为了显示全部的健康状态，NAP 客户端使用系统健康声明(SSoH)，包括 NAP 客户端的版本信息和 SHA 的 SoH 的设置。

当 NAP 客户端验证自己的系统健康时，为了通过 NAP 强制点评价，NAP 客户端会将 SSoH 传递给 NAP 健康策略服务器。NAP 健康策略服务器使用 SSoH 和健康要求策略来确定 NAP 客户端是否符合系统健康要求，如果不符合，那么将会进行修正使其变为符合。每个 SHV 都会产生一个健康声明响应(SoHR)，其中包含修正说明。例如，对于反病毒程序的 SoHR 包含当前反病毒签名文件的版本号和反病毒签名文件服务器的名称或 IP 地址。

根据来自 SHV 的 SoHR 和配置的健康要求策略，NAP 健康策略服务器创建一个健康响应系统声明(SSoHR)，显示 NAP 客户端是否符合，以及是否包含来自 SHV 的一系列 SoHR。NAP 健康策略服务器通过 NAP 强制点将 SSoHR 传递给 NAP 客户端。NAP 客户端将 SoHR 传递给 SHA。不符合的 SHA 自动修正其健康状态，并创建更新 SoH，然后健康验证进程将会再次启动。

13.2.2　强制客户端和服务器

NAP 强制客户端(EC)是 NAP 客户端的组成部分，该 NAP 客户端请求访问网络，将计算机健康状态传送到 NAP 强制点，并且为 NAP 客户端基础结构中的其他部分提供健康评估信息。NAP 平台的 NAP EC 在 Windows Vista、Windows XP SP3 和 Windows Server 2008 中的应用如下：

- 提供 IPSec 保护通信的 IPSec EC。
- 提供 802.1X 身份验证连接的 EAPHost EC。
- 提供远程访问 VPN 连接的 VPN EC。
- 提供基于 DHCP IPv4 地址配置的 DHCP EC。
- 提供到 TS 网关服务器的 TS 网关 EC。

NAP 强制服务器(ES)是运行 Windows Server 2008 的 NAP 强制点的一部分，可以通过 NAP 客户端健康状态到达 NPS 进行评估，并且根据 NPS 的响应，可以提供受限网络访问的强制。在 Windows Server 2008 中的 NAP ES 包含如下几类：

- 提供 IPSec 保护通信的 IPSec ES。
- 提供基于 DHCP IPv4 地址配置的 DHCP ES。
- 提供到 TS 网关服务器的 TS 网关 ES。

对于 802.1X 身份验证和远程访问 VPN 连接，在 802.1X 交换机或无线 AP 或 VPN 服务器上都没有独立的 ES 组件。

对于特定类型的网络访问或通信，不符合的计算机的 EC 和 ES 都需要健康状态验证和强制受限网络访问。

13.2.3　NPS

NPS 在 Windows Server 2008 中是 RADIUS 服务器和代理。作为 RADIUS 服务器，NPS 为各种类型的网络访问提供 AAA 服务。对于身份验证和授权，NPS 使用活动目录来检验用户或计算机的证书，并且当计算机尝试 802.1X 身份验证连接或 VPN 连接时，获取用户或计算机的账户属性。

NPS 也可作为 NAP 健康策略服务器，管理员可以在 NAP 健康策略服务器的健康要求策略中设置系统健康要求。NAP 健康策略服务器评价 NAP 客户端提供的健康状态信息来确定健康符合性，并且对于不符合的，修正设置可以使得 NAP 客户端变为符合的。

作为 AAA 服务器的 NPS 角色是独立于 NAP 健康策略服务器的角色的，这些角色根据需要可以单独使用，也可以联合使用。例如下面几种情况：

- 在没有配置 NAP 的内网中，NPS 可以是 AAA 服务器。
- 在配置了 802.1X 身份验证连接 NAP 的网络中，NPS 可以联合 AAA 服务器和健康策略服务器。
- 在配置了 DHCP 设置的 NAP 的内网中，NPS 可以是健康策略服务器。

13.2.4　网络访问保护策略的模式

在实际应用中，可以根据需要选择合适的策略模式，决定安全策略如何以策略中的配置文件评估客户

端、制作 NAC Manager 中的通报信息，并判定是否向用户发送信息、进行校正或采取强制执行策略等。网络访问保护策略的模式包括如下三种。

- Report Only(仅报告)：在该模式下，安全策略会以配置文件对客户端进行评估，而在 NAC Manager 内会制作报告信息，但在客户端点上不会显示任何信息，并进行校正动作，并且强制执行动作也不会执行。
- Remediate (校正)：在该模式下，安全策略会以配置文件对客户端进行评估，而在 NAC Manager 内会制作报告信息，并在客户端上显示信息，并执行校正动作，而存取样本也会依适当的存取或策略状态而套用。
- Enforce (强制执行)：在该模式下，安全策略会以配置文件对客户端进行评估，而在 NAC Manager 内会制作报告信息，并在客户端上显示信息，并执行校正动作，而存取样本也会依适当的存取或策略状态而套用。

13.3 强 制 方 式

Windows Vista、Windows XP SP3 和 Windows Server 2008 中的 NAP 支持如下类型的网络访问和通信：

- IPSec 保护通讯
- IEEE 802.1X 身份验证的网络连接
- 远程访问 VPN 连接
- DHCP 地址配置

Windows Server 2008 和 Windows Vista 还包含支持连接到 TS 网关服务器的 NAP。管理员可以使用这些类型的网络访问或通信，也称作 NAP 强制方式，独立或共同限制不符合计算机的访问或通信。

13.3.1 IPSec 强制

使用 IPSec 强制，计算机必须符合使用内网中服务器隔离或域隔离的其他符合计算机初始化的通信，这就要求入站通信受到 IPSec 的保护。因为 IPSec 强制利用 IPSec，用户可以为受保护的通信在每个 IP 或每个 TCP/UDP 端口号上指定要求。IPSec 强制在成功连接和获取有效 IP 地址配置后，为符合的计算机限制通信。IPSec 强制是 NAP 中限制网络访问或通信的最强形式之一。

IPSec 组件包括运行于 Windows Server 2008 的 HRA 上的 IPSec ES 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 上的 IPSec EC。当 NAP 客户端证明符合要求时，HRA 包含基于 X.509 健康证书。当 NAP 客户端使用其他符合的 NAP 客户端初始化 IPSec 保护的通信时，这些健康证书需要与 IPSec 策略设置一同来验证 NAP 客户端。

13.3.2 802.1X 强制

使用 802.1X 强制，计算机必须可以通过 802.1X 身份验证的网络连接来获取不受限的网络访问，网络连接包括认证的以太网交换机或 IEEE 802.1X 无线 AP。对于不符合的计算机，通过以太网交换机或无线 AP 中的受限访问配置文件来限制网络访问。受限访问配置文件可以指定访问控制列表(ACL)，必须符合以太网交换机或无线 AP 上配置的 IP 数据包过滤器的设置，或者符合受限网络 VLAN ID。使用 802.1X 强制，健康

策略要求在每次计算机尝试 802.1X 身份验证网络连接时都要进行强制。802.1X 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时应用受限访问配置文件到连接上。

802.1X 强制组件包括 Windows Server 2008 中的 NPS 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 上的 EAPHost EC。802.1X 为所有通过 802.1X 身份验证连接访问网络的计算机提供受限的网络访问。

13.3.3 VPN 强制

使用 VPN 强制，计算机必须可以通过远程访问 VPN 连接获取不受限的网络访问。对于符合的计算机，通过 VPN 服务器应用在 VPN 连接上的 IP 数据包过滤器的设置来限制网络访问。使用 VPN 强制，健康策略要求在每次计算机尝试获取远程访问 VPN 连接时，都要进行强制。VPN 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时，为到 VPN 连接的受限网络访问应用 IP 数据包过滤器。

VPN 强制组件包括 Windows Server 2008 中的 NPS 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 远程访问客户端上的 VPN EC。VPN 强制为所有通过远程访问 VPN 连接访问网络的计算机提供受限的网络访问。

13.3.4 DHCP 强制

使用 DHCP 强制，计算机必须可以从 DHCP 服务器上，获取受限网络访问的 IPv4 地址配置。对于不符合的计算机，网络访问受到 IPv4 地址配置的限制，该配置只允许到受限网络的访问。使用 DHCP 强制，健康策略要求在每次 DHCP 客户端尝试租借或续借 IPv4 地址配置时都要进行强制。DHCP 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时，只允许访问受限网络续借 IPv4 地址配置。

DHCP 强制组件包括 Windows Server 2008 DHCP 服务器中的 DHCP ES 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 DHCP 客户端中的 DHCP EC。因为 DHCP 强制依赖于受限 IPv4 地址配置，可以被管理员任意修改，所以该强制是 NAP 中受限网络访问中较弱的形式。

13.4 NAP 工作方式

管理员可以配置 NAP 使其满足网络的需要，所以，实际中的 NAP 配置是根据管理员的要求不断变化的。但 NAP 基本的操作大致是相同的，图 13-1 所示的内网的配置如下：

- 健康状态验证、健康策略符合性，以及对不符合的 NAP 客户端的受限网络访问。
- IPSec 强制、802.1X 强制、VPN 强制和 DHCP 强制。

当获取健康证书时，使用 802.1X 身份验证或 VPN 连接到内网，或者从 DHCP 服务器租借或续借 IPv4 地址配置，每个 NAP 客户端必须符合如下类别之一：

- 满足健康策略要求的 NAP 客户端归为符合类，并且允许不受限访问内网。
- 不满足健康策略要求的 NAP 客户端归为不符合类，只能访问受限网络直至满足要求为止。不符合的 NAP 客户端不能对内网产生病毒或其他类型的威胁，但是也不能获取软件更新或健康策略要求的配置。不符合的 NAP 客户端处于高度危险之中，并将危险传递到内网。NAP 客户端上的 SHA

可以自动更新计算机软件或不受限访问要求的设置。自动修正保证不符合的 NAP 客户端，获取必要的更新和尽快地授权不受限访问。

图 13-1 所示的内网包括受限网络，可以是逻辑创建或物理创建的。例如，IP 过滤器、静态路由、ACL 或 VLAN 标识都可以置于 NAP 客户端中，用来指定可以连接的修正服务器。在大部分局域网中，都会包含计算机和设备的不同组合，需要从健康策略要求中免除部分计算机或设备。例如，运行 Windows Server 2003、Windows 2000 或更老版本的 Windows 的计算机，这些操作系统根本不支持 NAP，为了防止这些计算机的受限访问，可以有选择地配置健康要求策略，为不支持 NAP 的计算机授权不受限访问。理论上，用户应该升级或更新不支持 NAP 的计算机，使其支持 NAP，保证所有计算机都可以进行系统健康评价。

13.4.1 IPSec 强制的工作方式

在如图 13-1 所示的企业网的 NAP 客户端上，执行 IPSec 强制的步骤如下。

① IPSec EC 组件发送 SSoH 到 HRA，说明自己当前的健康状态。

② HRA 发送 NAP 客户端的 SSoH 到 NAP 健康策略服务器。

③ 如果 NAP 客户端不符合，SSoHR 包含健康修正指示。

④ 如果健康状态符合，HRA 获取 NAP 客户端的健康证书。根据管理员配置的 IPSec 策略设置，NAP 客户端可以与其他符合的计算机进行 IPSec 保护的通信，使用健康证书进行 IPSec 身份验证，并且其他符合的计算机会回应启动的通信，使用自己的健康证书进行验证。

⑤ 如果健康状态不符合，HRA 发送 SSoHR 到 NAP 客户端，并且不颁发健康证书。NAP 客户端则不能使用其他计算机要求的健康证书进行身份验证启动通信。但是，NAP 客户端可以使用修正服务器来更正自己的健康状态。

⑥ NAP 客户端发送更新请求到适当的修正服务器。

⑦ 修正服务器为 NAP 客户端提供需要的符合性更新，NAP 客户端更新自己的 SSoH。

⑧ NAP 客户端发送自己更新后的 SSoH 到 HRA。

⑨ 如果所有需要的更新都已完成，NAP 健康策略服务器确定 NAP 客户端是符合的，并发送 SSoHR 到 HRA 指明其健康符合性。

⑩ HRA 获取 NAP 客户端的健康证书。NAP 客户端现在即可与其他符合的计算机进行 IPSec 保护的通信。

13.4.2 802.1X 强制的工作

在如图 13-1 所示的企业网中启用 802.1X 认证连接的 NAD 客户端上，执行 802.1X 强制的步骤如下。

① NAP 客户端和以太网交换机或无线 AP 启动 802.1X 身份验证。

② NAP 客户端发送用户或计算机的认证证书到 NAP 健康策略服务器。

③ 如果认证证书有效，NAP 健康策略服务器向 NAP 客户端发送健康状态请求；如果认证证书无效，那么该连接将结束。

④ NAP 客户端发送自己的 SSoH 到 NAP 健康策略服务器。

⑤ NAP 健康策略服务器评估 NAP 客户端的 SSoH，确定 NAP 客户端是否符合，并且将结果发送到 NAP 客户端和以太网交换机或无线 AP。如果 NAP 客户端不符合，结果中包含以太网交换机或无线 AP 的受限访问配置文件，SSoHR 包括 NAP 客户端的健康修正指示。

⑥ 如果健康状态符合，以太网交换机或无线 AP 完成 802.1X 身份验证，NAP 客户端可以不受限地访

问内网。

⑦ 如果健康状态不符合，以太网交换机或无线 AP 完成 802.1X 身份验证，但是通过 ACL 或 VLAN ID 限制 NAP 客户端的访问。NAP 客户端只可以发送通讯到内网中的修正服务器。

⑧ NAP 客户端发送更新请求到适当的修正服务器。

⑨ 修正服务器为 NAP 客户端提供需要的符合性更新。NAP 客户端更新自己的 SSoH。

⑩ NAP 客户端重新进行 802.1X 身份验证，并发送自己的更新后的 SSoH 到 NAP 健康策略服务器。

⑪ 如果所有需要的更新都已完成，NAP 健康策略服务器确定 NAP 客户端是符合的，并指示以太网交换机或无线 AP 允许不受限访问。

⑫ 以太网交换机或无线 AP 完成 802.1X 身份验证，NAP 客户端可以不受限地访问内网。

13.4.3 VPN 强制的工作

在如图 13-1 所示的企业网中启用 VPN 连接的 NAP 客户端上，执行 VPN 强制的步骤如下。

① NAP 客户端启动连接到 VPN 服务器。

② NAP 客户端发送用户认证证书到 VPN 服务器。

③ 如果证书有效，NAP 健康策略服务器向 NAP 客户端发送健康状态请求；如果认证证书无效，那么该 VPN 连接尝试结束。

④ NAP 客户端发送自己的 SSoH 到 NAP 健康策略服务器。

⑤ NAP 健康策略服务器评估 NAP 客户端的 SSoH，确定 NAP 客户端是否符合，并且将结果发送到 NAP 客户端和 VPN 服务器。如果 NAP 客户端不符合，结果包含 VPN 服务器的 IP 数据包过滤器的设置，SSoHR 包括 NAP 客户端的健康修正指示。

⑥ 如果健康状态符合，VPN 服务器完成 VPN 连接，NAP 客户端可以不受限访问内网。

⑦ 如果健康状态不符合，VPN 服务器完成 VPN 连接，但是根据数据包过滤器限制 NAP 客户端的访问。NAP 客户端只可以发送通讯到内网中的修正服务器。

⑧ NAP 客户端发送更新请求到适当的修正服务器。

⑨ 修正服务器为 NAP 客户端提供需要的符合性更新，NAP 客户端更新自己的 SSoH。

⑩ NAP 客户端重新进行 VPN 服务器的身份验证，并发送自己的更新后的 SSoH 到 NAP 健康策略服务器。

⑪ 如果所有需要的更新都已完成，NAP 健康策略服务器确定 NAP 客户端是符合的，并指示 VPN 服务器允许不受限访问。

⑫ VPN 服务器完成 VPN 连接，NAP 客户端可以不受限地访问内网。

13.4.4 DHCP 强制的工作

在如图 13-1 所示的企业网上尝试初始 DHCP 配置的 NAD 客户端上，执行 DHCP 强制的步骤如下。

① NAP 客户端发送包含 SSoH 的 DHCP 请求消息到 DHCP 服务器。

② DHCP 服务器发送 NAP 客户端的 SSoH 到 NAP 健康策略服务器。

③ NAP 健康策略服务器评估 NAP 客户端的 SSoH，确定 NAP 客户端是否符合，并且将结果发送到 DHCP 服务器。如果 NAP 客户端不符合，结果包含 DHCP 服务器的受限访问配置设置，SSoHR 包括 NAP 客户端的健康修正指示。

④ 如果健康状态符合，DHCP 服务器为 NAP 客户端不受限访问分配 IPv4 地址，并且完成 DHCP 消息

交换。

⑤ 如果健康状态不符合，DHCP 服务器为 NAP 客户端访问受限网络分配 IPv4 地址，并完成 DHCP 消息交换，发送 SSoHR 到 NAP 客户端。NAP 客户端只可以发送通讯到内网中的修正服务器。

⑥ NAP 客户端发送更新请求到适当的修正服务器。

⑦ 修正服务器为 NAP 客户端提供需要的符合性更新，NAP 客户端更新自己的 SSoH。

⑧ NAP 客户端发送包含更新后的 SSoH 的 DHCP 请求消息到 DHCP 服务器。

⑨ DHCP 服务器发送 NAP 客户端更新过的 SSoH 到 NAP 健康策略服务器。

⑩ 如果所有需要的更新都已完成，NAP 健康策略服务器确定 NAP 客户端是符合的，并指示 DHCP 服务器为不受限访问内网的 NAP 客户端分配 IPv4 地址。

⑪ DHCP 服务器为 NAP 客户端不受限访问分配 IPv4 地址，并且完成 DHCP 消息交换。

13.5 网络访问保护的准备

在网络访问保护(NAP)前，需要进行一些准备工作，包括评价当前的网络基础结构和配置独立于 NAP 强制方式的 NAP 组件的设计。在正式进行部署前，需要用户理解基于 Windows 的身份验证基础结构的活动目录的角色、PKI、组策略和 RADIUS 及 NAP 组件与 NAP 强制方式等基本概念。

13.5.1 评价当前网络基础结构

在开始 NAP 配置之前，需要详细记录和评价当前网络基础结构，以保证其具有所需的主机和访问服务器，以及保证其满足支持 NAP 的要求。当前网络基础结构的评价可以分为内网计算机、附属内网的第 2 层和网络支持基础结构。

1. 内网计算机

内网计算机可以分为 NAP 客户端的候选对象和不支持 NAP 的客户端，也可以被分为可管理和不可管理两种。

(1) 可管理的计算机

可管理的计算机主要分为以下两种方式。

- 支持 NAP：包括运行 Windows Vista、Windows XP SP3 或 Windows Server 2008 的计算机，以及使用 NAP 客户端的其他操作系统。
- 不支持 NAP：包括运行不含有 NAP 客户端的操作系统的计算机。

802.1X 和 VPN 的 NAP 强制方式不需要为健康评估管理计算机，但是身份验证和授权计算机则需要被管理。对于 IPSec 的 NAP 强制方式，计算机可以不被管理，但推荐其接受管理。

(2) 不可管理的计算机

不可管理的计算机可以分为以下两种方式。

- 支持 NAP：包括运行 Windows Vista、Windows XP SP3 或 Windows Server 2008 的计算机，以及使用 NAP 客户端的其他操作系统。
- 不支持 NAP：包括运行不含有 NAP 客户端的操作系统的计算机。

2. 附属内网的第 2 层

另外一种计算机的分类是通过附属内网的第 2 层方式。对于有线连接内网的计算机，对桌面用户和服务器计算机，最常用的计算机分类如下。

- 使用 IEEE 802.1X 身份验证：使用 IEEE 802.1X 身份验证鉴别计算机交换端口的使用。如果用户想要使用 802.1X 强制方式，需要确保启用 802.1X 的计算机使用基于 PEAP 身份验证方式，例如 PEAP-MS-CHAP v2 或者 PEAP-TLS。因为系统健康信息是使用 PEAP 消息在有线 NAP 客户端和 NAP 健康策略服务器上传输的，所以需要基于 PEAP 的身份验证方式。如果启用 802.1X 的计算机使用 EAP-MD5-CHAP，则需要配置其使用 PEAP- MS-CHAP v2；如果启用 802.1X 的计算机使用 EAP-TLS，则需要配置其使用 PEAP-TLS。
- 不使用 802.1X 身份验证：如果用户想要使用 802.1X 强制方式，必须使用 PEAP- MS-CHAP v2 或者 PEAP-TLS 身份验证方式配置 802.1X 身份验证。

对于使用 IEEE 802.11 无线方式连接内网的计算机，最常用的计算机分类如下。

- 使用 IEEE 802.1X 身份验证：使用 WPA2-企业或 WPA-企业的 IEEE 802.1X 标准来认证无线访问点的无线连接的使用。如果用户想要使用 802.1X 强制方式，应确保使用 802.1X 的无线客户端计算机使用基于 PEAP 身份验证方式，例如 PEAP- MS-CHAP v2 或者 PEAP-TLS。因为系统健康信息是使用 PEAP 消息在无线 NAP 客户端和 NAP 健康策略服务器上传输的，所以需要基于 PEAP 的身份验证方式。如果无线客户端使用 EAP-TLS，则需要配置其使用 PEAP-TLS。
- 不使用 802.1X 身份验证：如果用户没有使用 WPA2-企业或 WPA-企业的 802.1X 身份验证，立即更新无线网络来保护内网，无论是否想使用 802.1X 强制方式。如果用户想要为无线连接使用 802.1X 强制方式，那么使用基于 PEAP- MS-CHAP v2 或者 PEAP-TLS 身份验证方式的 WPA2-企业或 WPA-企业。

对于使用远程连接内网的计算机，常用形式有便携式计算机从家庭中进行连接，用户可以根据远程访问连接是拨号或 VPN 连接进行分类。由于局域网高速连接的优点，使其发展迅速，对于不符合的计算机远程访问连接不服从于 NAP 健康评估和受限访问的强制。VPN 强制方式不包含拨号远程访问连接。如果用户想要确定所有连接到内网的第 2 层连接是否服从 NAP 健康评估，需要淘汰拨号远程访问连接。如果不能彻底消除拨号远程访问连接，可以尝试限制拨号远程访问，来降低来自不符合计算机对内网的威胁。

如果想要使用 VPN 强制方式，确保 VPN 客户端计算机正使用基于 PEAP 身份验证方式，例如 PEAP-MS-CHAP v2 或者 PEAP-TLS。因为系统健康信息是使用 PEAP 消息在 VPN 客户端和 NAP 健康策略服务器上传输的，所以需要基于 PEAP 的身份验证方式。

3. 网络支持基础结构

网络支持基础结构是一项在局域网启用网络的服务，具体内容包括如下。

- DHCP：如果想要在基于 Windows 的 DHCP 服务器上使用 DHCP 强制方式，必须更新 DHCP 服务器到 Windows Server 2008。
- DNS：根据如何为不符合的计算机执行受限访问，可能需要其他 DNS 服务器。
- WINS：根据如何为不符合的计算机执行受限访问，可能需要其他 WINS 服务器。
- 活动目录：活动目录域控制器不需要更新到 Windows Server 2008。但根据如何执行受限访问，可能需要其他活动目录域控制器。如果用户的域控制器运行的是 Windows Server 2008，应该为不符合的客户端使用只读域控制器(RODC)。RODC 是 Windows Server 2008 中的一种新型的域控

制器，可以配置于不能保障物理安全的位置。RODC 寄宿在活动目录数据库的只读部门。

- 组策略：组策略对象(GPO)可用于集中配置和传播 NAP 客户端设置到可管理的计算机。用户不需要使用 Windows Server 2008 的域控制器。如果所有域控制器运行的都是 Windows Server 2003，则必须在运行 Windows Vista 或 Windows Server 2008 的计算机的 GPO 上配置 NAP 客户端策略设置。
- IPSec：如果用户想要使用 IPSec 强制，必须使用连接安全规则的形式更新 IPSec 策略设置，在活动目录 GPO 的 IPSec 身份验证过程中使用健康证书。借助于 NAP 客户端的设置，则不需要使用基于 Windows Server 2008 的域控制器。如果所有域控制器都运行的是 Windows Server 2003，则必须在运行 Windows Vista 或 Windows Server 2008 的计算机的 GPO 上配置 IPSec 策略设置。
- PKI：如果想要使用 IPSec 强制，则必须配置 PKI 或修改现有的 PKI，使其包含基于 Windows 的健康证书颁发结构 CA。
- VPN：如果用户想要使用基于 Windows 的 VPN 服务器的 VPN 强制，则必须更新 VPN 服务器到 Windows Server 2008。
- RADIUS：如果用户没有 RADIUS 基础结构，必须配置基于 Windows Server 2008 的 RADIUS 服务器使用 NAP 强制方式中任意一种。如果用户拥有 RADIUS 基础结构，必须更新 RADIUS 服务器到 Windows Server 2008，为 NAP 健康策略评估使用网络策略服务器(NPS)。

13.5.2　相关服务组件的安装

不同类型的 NAP 强制，所需的网络组件有所不同，不仅需要相应的服务器角色，还需要提供辅助验证工作的组件，如证书服务器、域控制器等。通常情况，在网络中应用 NAP 强制之前，首先需要安装或配置相应的服务器角色，然后准备所需的网络环境。

1. 域控制器

域控制器的主要功能就是为内网用户和计算机提供基本的身份认证。在网络中部署和应用 NAP 强制之前，首先应在域中创建相应的用户账户或组，例如，NAP 免除安全组、测试用户组等。

NAP 免除安全组用于存储网络中的非 NAP 客户端，如 Windows Server 2003、Windows XP(非 SP3)系统用户等。这些用户无法应用各种 NAP 强制，管理员为符合安全策略和不符合安全策略的客户端设置访问权限后，必须单独为这些客户端指定是授权访问，还是限制访问。

测试用户组则用于存储广泛应用 NAP 强制之前的测试工作。不同的 NAP 强制分别限制不同类型的网络访问。如果由于应用了网络健康评估策略，而影响了正常的网络应用，就得不偿失了。因此，应用 NAP 强制之前必须在小范围内进行测试。

2. 证书服务器

数字证书是最常用的网络安全保护手段之一。在部署 NAP 强制的网络中，证书服务器的主要作用，就是为网络中的各种服务器角色或客户端颁发数字证书，实现彼此之间的身份验证。证书服务器在 IPSec 强制的网络中是必需的，而在其他 NAP 强制的网络中则是可选的。例如，在 VPN 强制网络中，如果用户选择了特定的加密传输协议和身份验证方式，则可能需要准备数字证书，验证 VPN 服务器和 VPN 客户端身份的有效性。

3. 网络策略服务器

网络策略服务器(NPS)是任何 NAP 强制都必需的，提供各种安全健康评估、记账等功能，它是 Windows

Server 2008 系统的新增功能之一。NPS 允许用户通过 RADIUS 服务器、RADIUS 代理和网络访问保护策略服务器，集中配置和管理网络策略。

(1) RADIUS 服务器

从 Windows Server 2008 系统开始，RADIUS 服务器已经被集成在 NPS 中。作为 RADIUS 服务器，NPS 为许多类型的网络访问(包括无线、身份验证切换、VPN 远程访问、路由器到路由器的连接)执行集中化的连接身份验证、授权和记账。

RADIUS 服务器具有对用户账户信息的访问权限，并可以检查网络访问身份验证凭据。如果用户的凭据是真实的，并且连接尝试获得授权，RADIUS 服务器将根据指定条件向用户授予访问权限，并将网络访问连接记录到记账日志中。使用 RADIUS 允许在一个中心位置(而不是在每台访问服务器上)收集并维护网络访问用户身份验证、授权和记账数据。

(2) RADIUS 代理

作为 RADIUS 代理，NPS 将身份验证和记账消息转发到其他 RADIUS 服务器。使用 NPS，各组织还可以在保留对用户身份验证、授权和记账活动控制的同时，将远程访问基础结构外包给服务提供商。

(3) NAP 策略服务器

NAP 包含在 Windows Vista 和 Windows Server 2008 中，并通过确保按照组织网络健康策略配置客户端计算机后才允许其连接到网络资源，从而有助于保护对专用网络的访问。此外，计算机连接到网络时，NAP 会监视客户端计算机对管理员定义的健康策略的遵从性情况。使用 NAP 自动更新，可以自动更新不符合要求的计算机，以使其遵从健康策略，从而使它们能够连接到网络。

系统管理员可以定义网络健康策略，并使用 NPS 中或其他公司(取决于 NAP 部署)提供的 NAP 组件创建这些策略。

健康策略可以包含软件要求、安全更新要求和所需的配置设置等内容。NAP 通过检查和评估客户端计算机的健康，在认为客户端计算机不健康时限制网络访问，以及修正不健康的客户端计算机以进行充分的网络访问，来强制运行健康策略。

13.5.3 更新服务器

当用户配置健康要求策略来强制受限访问时，更新服务器是不符合的 NAP 客户端可以访问的内网的子集。更新服务器包括网络基础结构服务器和健康更新服务器。不符合的 NAP 客户端，使用这些服务器或服务器上的资源来自动或手动执行更新。健康要求策略也可以为不支持 NAP 的客户端强制受限访问。

如果使用报告模式，则不需要更新服务器。在报告模式下，不符合的 NAP 客户端的访问不受限制。但是，为了避免不符合健康要求的计算机为内网带来的威胁，必须最终转换到强制模式，即需要建立更新服务器。

在 VPN 和 DHCP 模式下不符合的 NAP 客户端，可以访问的更新服务器列表，需要与 NAP 客户端健康评估匹配的网络策略的 NAP 强制设置中指定的更新服务器组相符合。更新服务器组是一个 IPv4 和 IPv6 地址的列表。该列表应该包括网络基础结构服务器和健康更新服务器。

基础结构服务器包括如下几个部分：

- DHCP 服务器，为不符合的 NAP 客户端分配 IPv4 地址和其他配置参数，保证其可以访问更新服务器。如果用户正使用 DHCP 强制方式，则不需要添加支持 NAP 的 DHCP 服务器作为更新服务器。

- DNS 和 WINS 服务器，为不符合的 NAP 客户端提供名称解析，保证其可以解析名称，并访问其他更新服务器。
- 活动目录域控制器，保证不符合的 NAP 客户端可以执行域登录，访问基于域的资源，如文件共享。
- Internet 代理服务器，保证不符合的 NAP 客户端可以访问 Internet。
- HRA，保证不符合的 NAP 客户端可以在 IPSec 强制模式下获取健康证书。
- 更新 NAP 客户端系统健康需要健康更新服务器，包括如下几个部分。
  - 疑难解答 URL 服务器：在“更新服务器和疑难解答 URL”对话框中的疑难解答 URL 文本框中，指定 Web 服务器。
  - 反病毒更新服务器：这些服务器可能位于 Internet 上。如果用户拥有 Internet 代理服务器作为更新服务器，则不需要包含基于 Internet 的反病毒更新服务器。如果在内网中拥有反病毒更新服务器，则应该将其作为更新服务器，因为在尝试连接访问基于 Internet 的反病毒服务器前，通常会首先在这些服务器上检查更新。
  - 反间谍更新服务器：如同反病毒服务器一样，如果在内网中配置了反间谍更新服务器，则需将其作为更新服务器。如果只存在于 Internet 上，确保 Internet 代理服务器包含在更新服务器组中。
  - 软件更新服务器：如同反病毒服务器一样，如果在内网中配置了软件更新服务器，则需将其作为更新服务器。如果只存在于 Internet 上，确保 Internet 代理服务器包含在更新服务器组中。

更新 NAP 客户端所需要的健康更新服务器的设置依赖于用于健康评估的 SHV。

13.5.4　安装 NPS

在 Active Directory 环境中部署 NAP 系统，用户可以更充分地使用其提供的网络访问保护功能。客户端可以是 Windows Server 2008、Windows Vista 或 Windows XP SP3 系统，同时确保已加入域。默认安装完成 Windows Server 2008 后，没有安装网络策略和远程访问服务，需要网络用户手动安装该服务。

① 运行“添加角色向导”，在“选择服务器角色”界面中，选中“网络策略和访问服务”复选框，如图 13-2 所示。

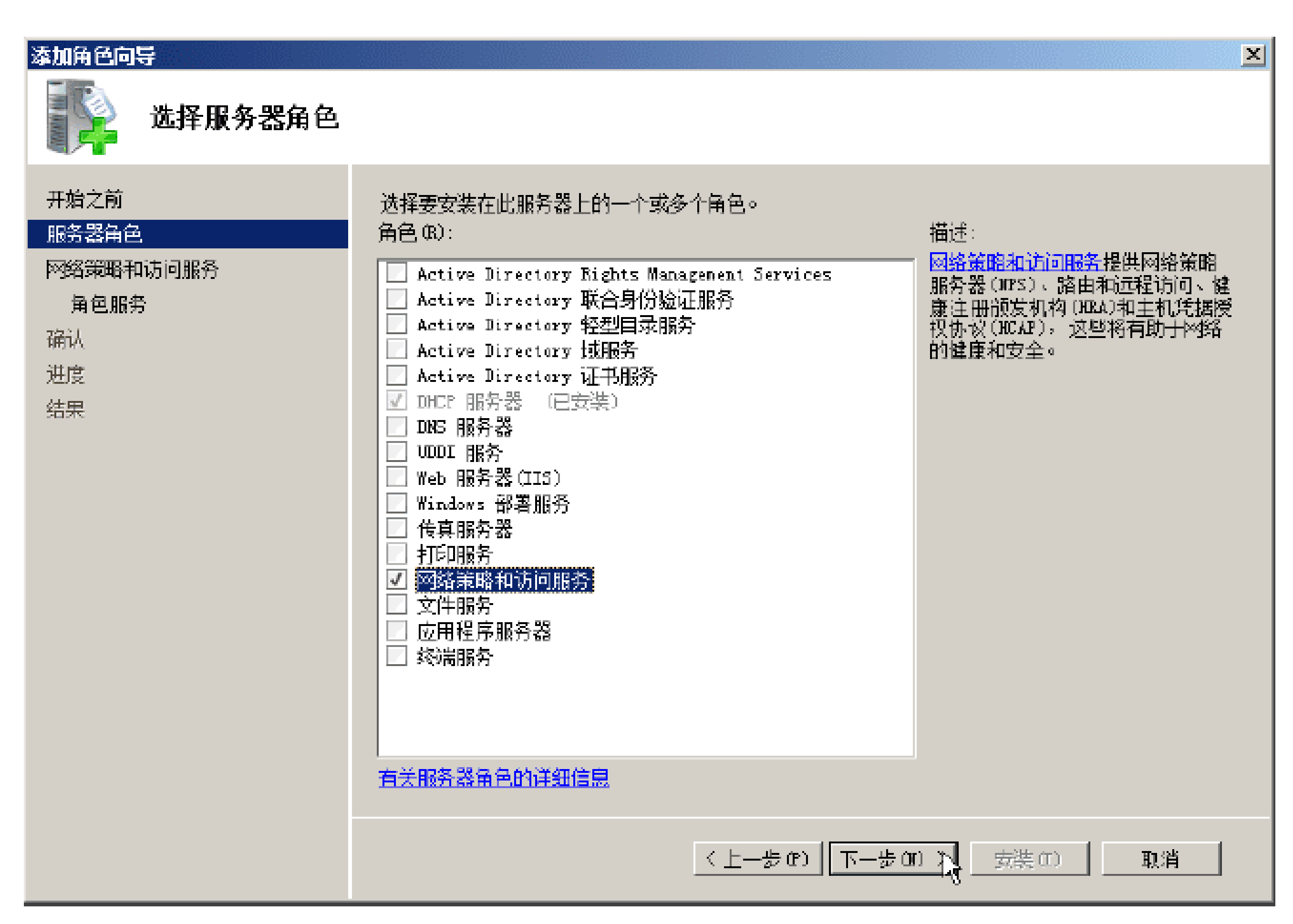


图 13-2　“选择服务器角色”界面

② 单击“下一步”按钮，显示如图 13-3 所示的“网络策略和访问服务”界面。其中概要介绍了“网络策略和访问服务”完成的功能，单击“其他信息”中的链接可以查看详细帮助文件。



图 13-3 “网络策略和访问服务”界面

③ 单击“下一步”按钮，显示如图 13-4 所示的“选择角色服务”界面。在“角色服务”列表中，选中“网络策略服务器”复选框。



图 13-4 “选择角色服务”界面



提示：本文中设计的案例只是网络访问保护系统的一个简单应用，适用于大多数网络环境。角色服务中的“路由和远程访问服务”、“健康注册机构”和 Host Credential Authorization Protocol，只有在特殊环境中才会用到，这里不作选择。需要注意的是，选择这些角色后，需要添加相应的角色服务和功能组件，如选择“健康注册机构”角色，就需要安装 Active Directory 证书服务、Web 服务器等。

④ 单击“下一步”按钮，显示如图 13-5 所示的“确认安装选择”界面。其中列出了已选择安装的服务设置信息。

⑤　单击“安装”按钮，开始安装选择的服务。安装完成后，显示如图 13-6 所示的“安装结果”界面。

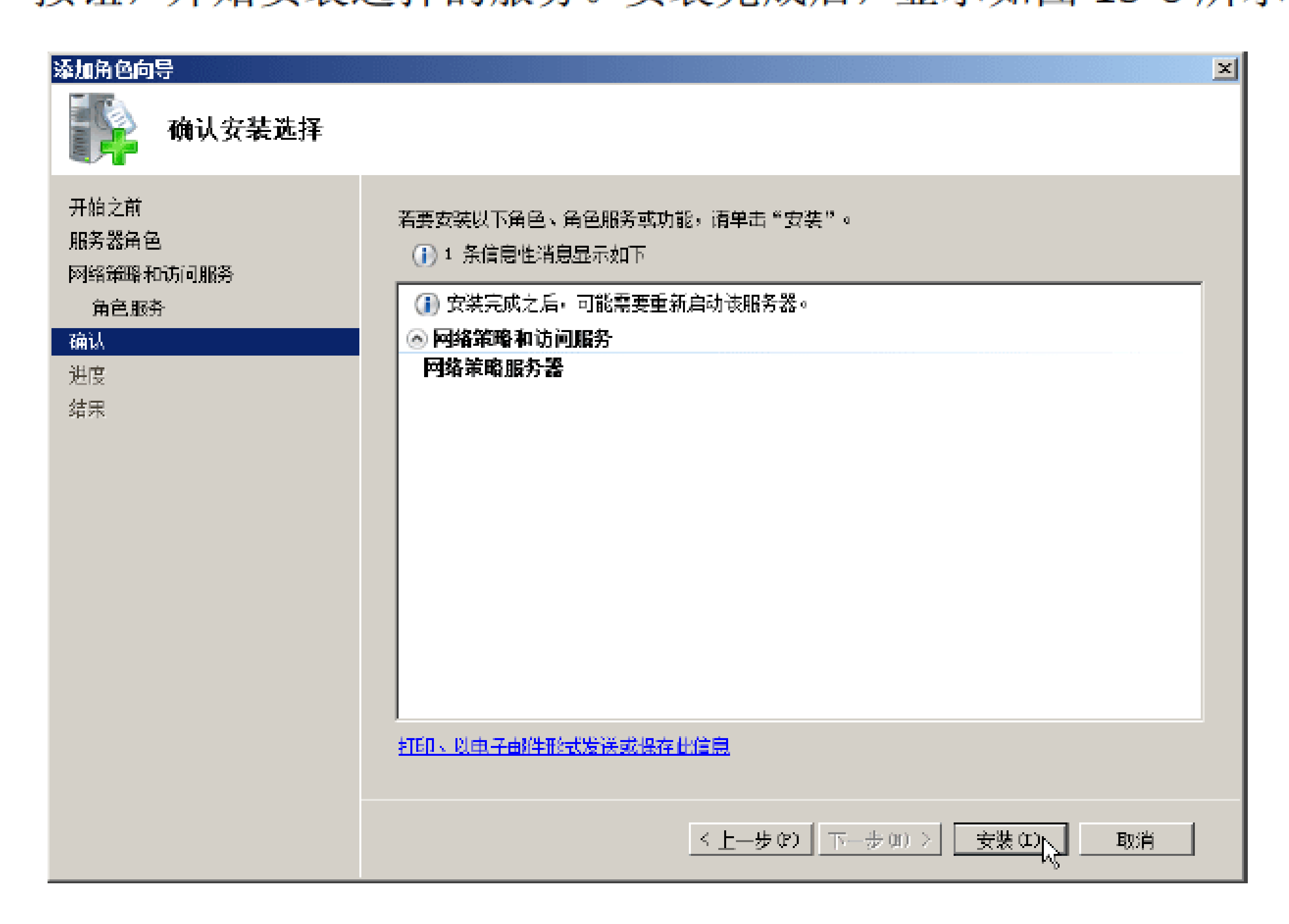


图 13-5　“确认安装选择”界面



图 13-6　“安装结果”界面

⑥　单击“关闭”按钮，完成“网络策略和访问服务”的安装。

13.5.5　NAP 健康策略服务器

NAP 执行健康评估的中心服务器是运行 NPS 的计算机，也称作 NAP 健康策略服务器。这里运行 NPS 的计算机是作为 RADIUS 服务器，从 NAP 强制点(RADIUS 客户端)接收 RADIUS 访问请求消息，其中 NAP 强制点包括健康注册机构(HRA)、802.11 无线访问点、802.1X 交换机、支持 NAP 的 VPN 服务器，以及支持 NAP 的 DHCP 服务器。

1. 计划和设计的考虑

当配置 NAP 健康策略服务器时，必须考虑如下计划和设计的问题：

- 现有 RADIUS 基础结构
- RADIUS 服务器的容量
- NPS 日志和报告模式
- 分支结构
- 系统健康的有效性

(1) 现有 RADIUS 基础结构

如果用户已有运行 Windows Server 2003 或 Windows Server 2008 和 IAS 的 RADIUS 服务器，则必须在现有 RADIUS 服务器上更新 Windows Server 2008，并且作为 NAP 健康策略服务器进行配置。

如果用户现有 RADIUS 服务器运行除了 Windows Server 2003 或 Windows Server 2008 以外的操作系统，那么这些服务器就不能更新支持 NPS 和 NAP 健康评估。用户必须配置运行 Windows Server 2008 的独立计算机和 NPS 作为 NAP 健康策略服务器。

如果用户没有 RADIUS 基础结构，必须在新计算机或现有计算机上安装 Windows Server 2008 和 NPS。例如，如果内网没有为有线连接、802.11 无线连接或 VPN 连接使用 802.1X 身份验证，则不需要 RADIUS 服务器。但当用户配置 NAP 时，无论使用哪种 NAP 强制方式，都需要 RADIUS 基础结构执行健康评估。

(2) RADIUS 服务器容量

对于现有的 RADIUS 基础结构，大部分情况下，用户可以为 NAP 健康评估使用与第 2 层身份验证、授权和记账相同的 RADIUS 服务器。在大部分情况下，不需要添加其他 RADIUS 服务器到 RADIUS 基础结构中。

如果用户没有 RADIUS 基础结构，可以配置两台 NAP 健康策略服务器，使用主 RADIUS 服务器和备用 RADIUS 服务器配置 NAP 强制点，在两台 NAP 健康策略服务器间分担负载。

如果需要提高 RADIUS 容量，以及在多个 RADIUS 服务器间均衡负载，可以在 NAP 强制点和 NAP 健康策略服务器间配置 RADIUS 代理层。

(3) NPS 日志和报告模式

NPS 服务日志入站 RADIUS 请求是到本地文件还是到本地文件和运行 Microsoft SQL Server 的计算机，具体取决于如何为日志记录配置 NPS。NPS 日志对于 NAP 配置十分重要，因为用户可以在局域网中，以报告模式配置 NAP，检查健康符合性，但是没有强制受限网络访问，并且没有通知用户其计算机与系统健康要求不符合。在报告模式中，可以分析日志信息来确定如下方面：

- 局域网中哪些计算机启用了 NAP。
- 支持 NAP 的计算机中，哪些是符合的。

用户可以使用该信息来配置支持 NAP 的计算机变为符合。报告模式运行用户在启用强制模式之前调整 NAP 的配置，这样不符合和不支持 NAP 的客户端的访问会受到限制，并且 NAP 客户端的用户会被通知计算机与系统健康要求不符合。

(4) 分支机构

在分支机构网络中，配置执行 NAP 健康评估的 NPS 服务器，主要取决于该分支结构是否拥有现成的活动目录域控制器：

- 如果分支机构拥有现成的活动目录域控制器，可以在分支结构的至少两台域控制器上安装 NPS，分支结构的 NAP 强制点用其作为 NAP 健康策略服务器。
- 如果分支结构不存在现成的活动目录域控制器，不需要在分支结构的服务器上安装 NPS。只需要

NAP 强制点使用 RADIUS 服务器。

- 如果分支结构没有现成的活动目录域控制器，也可以在分支结构中配置基于 NAP 的 RADIUS 代理，使用 RADIUS 服务器。

(5) 系统健康的有效性

NPS 的健康策略设置允许用户定义健康符合性和不符合性，这种定义以安装在 NAP 健康策略服务器的系统健康有效性(SHV)的形式进行。NAP 健康策略服务器的 SHV 验证 NAP 客户端的系统健康代理(SHA)发出的系统健康状态是否符合一种或多种系统健康属性。SHV 也可以执行 NAP 客户端系统健康的评估，NAP 客户端健康的评估结果将被发送到 NPS 服务来匹配网络策略和健康策略。

Windows Server 2008 包含 Windows 安全健康有效性、对应 Windows 安全健康代理的 SHV。使用 Windows 安全健康代理和 Windows 安全健康有效性，可以为 Windows Vista 和 Windows XP SP3 的 Windows 安全中心的系统服务定义系统健康要求。

除了内嵌的 Windows 安全健康有效性 SHV，用户将需要确定为 NAP 客户端定义系统健康要求的其他 SHV。其他 SHV 可能从提供商处获取，支持第三方主机防火墙、防毒软件、反间谍软件、入侵检测系统和其他安全软件。

2. 配置步骤

为了配置 NAP 健康策略服务器，需要完成如下任务：

- 如果需要，可以配置基于 NPS 的 RADIUS 服务器。
- 指定哪个 RADIUS 服务器是 NAP 健康策略服务器。
- 如果需要，可以在 RADIUS 服务器上为 NAP 强制点添加 RADIUS 客户端。例如，如果无线 AP、身份验证交换机和 VPN 服务器的 RADIUS 客户端已经配置完成，并且用户不想使用 IPSec 或 DHCP 强制，那么 NAP 健康策略服务器不需要配置其他 RADIUS 客户端。但是，如果用户计划使用 IPSec 或 DHCP 强制方式，则必须添加符合 HRA 和 DHCP 服务器的 RADIUS 客户端。
- 根据需要，在 NPS 健康策略服务器上为健康评估安装和配置 SHV。
- 根据需要使用“配置 NAP 向导”配置 NAP 健康要求策略。

3. 运行维护

NAP 健康策略服务器的维护工作包括：NAP 强制点的 RADIUS 客户端的管理和 SHV 健康要求策略的管理。

(1) 为 NAP 强制点管理 RADIUS 客户端

当用户配置新的 NAP 强制点时，如新的无线 AP 或 VPN 服务器，必须完成如下工作：

- 将 RADIUS 客户端添加 NAP 强制点到 NPS 健康策略服务器上。
- 配置 NAP 强制点，使其使用 NAP 健康策略服务器作为 RADIUS 服务器。

当用户移除 NAP 强制点时，在 NAP 健康策略服务器上删除 NAP 强制点作为 RADIUS 客户端。

(2) 为 SHV 管理健康要求策略

当用户在健康要求策略中有新的 SHV 时，必须完成如下工作：

- 根据需要，在 NAP 客户端上安装相应的 SHA。
- 在 NAP 健康策略服务器上安装 SHV。

- 为了 SHV 配置健康要求，并配置健康策略，使新的 SHV 包含在系统健康评估中。

当用户想要移除 SHV 时，需要完成如下工作。

- 配置健康策略，使其不再在系统健康评估中包含新的 SHV。
- 从 NPS 健康策略服务器上移除 SHV。
- 从 NAP 客户端上移除相应的 SHA。

13.5.6 健康要求策略配置

NAP 健康策略服务器上的健康要求策略，决定支持 NAP 的客户端是否符合，如何处理不符合的 NAP 客户端，以及是否应该自动修正它们的健康状态，和如何处理不支持 NAP 的客户端。

1. 健康要求策略的组件

健康要求策略的组成部分包括连接请求策略、健康策略、网络策略和 NAP 设置。

(1) 连接请求策略

连接请求策略是一种规则的指令组，允许 NPS 服务确定 RADIUS 客户端是否有指定的连接尝试或记账消息，被发送到另一个 RADIUS 服务器，用户可以在网络策略服务器管理单元中“策略\连接请求策略”节点配置连接请求策略。当发送消息时，可以连接请求策略指定的远程 RADIUS 服务器组，并可在“网络策略服务器”管理单元中的“RADIUS 客户端和服务器\远程 RADIUS 服务器组”节点中进行配置。

当配置 NPS 服务器执行 NAP 健康评估时，NPS 即为 RADIUS 服务器，所以不需要远程 RADIUS 服务器组。但是，RADIUS 请求消息的本地处理的连接请求策略，需要为 NAP 健康评估进行配置或定制。

(2) 健康策略

健康策略允许用户在安装 SHV 的条件下指定健康要求，以及 NAP 客户端是否必须通过或未通过所有选择的 SHV。如图 13-7 所示为健康策略的示例。

在“策略名称”文本框中，输入策略的唯一名称。在“客户端 SHV 检查”下拉列表中，可以根据需要选择如下内容。

- 客户端通过了所有 SHV 检查：在连接请求中的客户端健康状态，必须通过所有 SHV 的健康要求。
- 客户端未能通过所有 SHV 检查：在连接请求中的客户端健康状态，必须未通过所有 SHV 的健康要求。
- 客户端通过一个或多个 SHV 检查：连接请求中的客户端健康状态，必须至少通过一个 SHV 的健康要求。
- 客户端未能通过一个或多个 SHV 检查：连接请求中的客户端健康状态，必须未通过至少一个 SHV 的健康要求。

在“此健康策略中使用的 SHV”列表框中，选择已安装的应用于策略的 SHV。默认情况下，“Windows 安全健康验证程序”已显示在列表中。

(3) 网络访问保护设置

在“网络策略服务器”控制台中，在“网络访问保护”节点中的网络访问保护设置，包括系统健康验证器和更新服务器组。系统健康验证器为健康要求和错误条件指定 SHV 的配置。更新服务器组为网络访问受限的不符合的客户端，在 DHCP 和 VPN 强制方式下指定可用的服务器组。

■　系统健康验证器

在系统健康验证器节点，显示了安装在 NPS 服务器上的 SHV 的设置，允许用户为健康要求和错误条件配置这些设置。默认情况下，Windows 安全健康验证程序已经安装，如图 13-8 所示为“Windows 安全健康验证程序 属性”对话框。

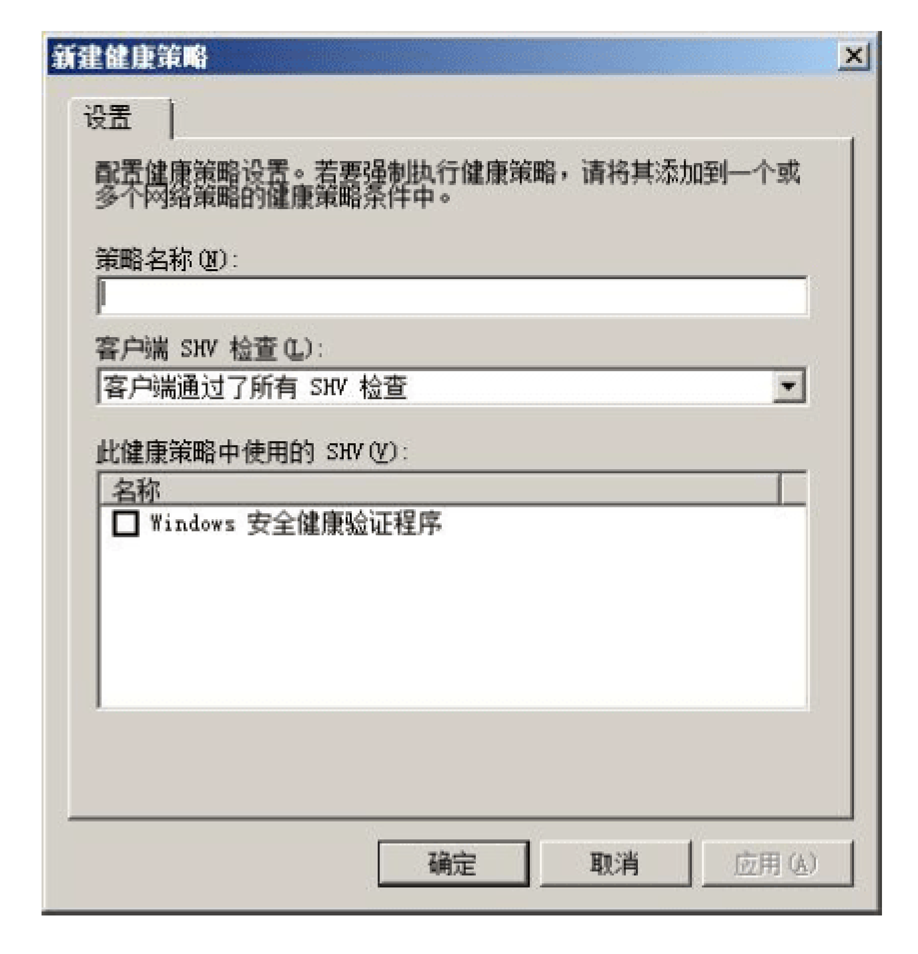



图 13-7　健康策略的示例

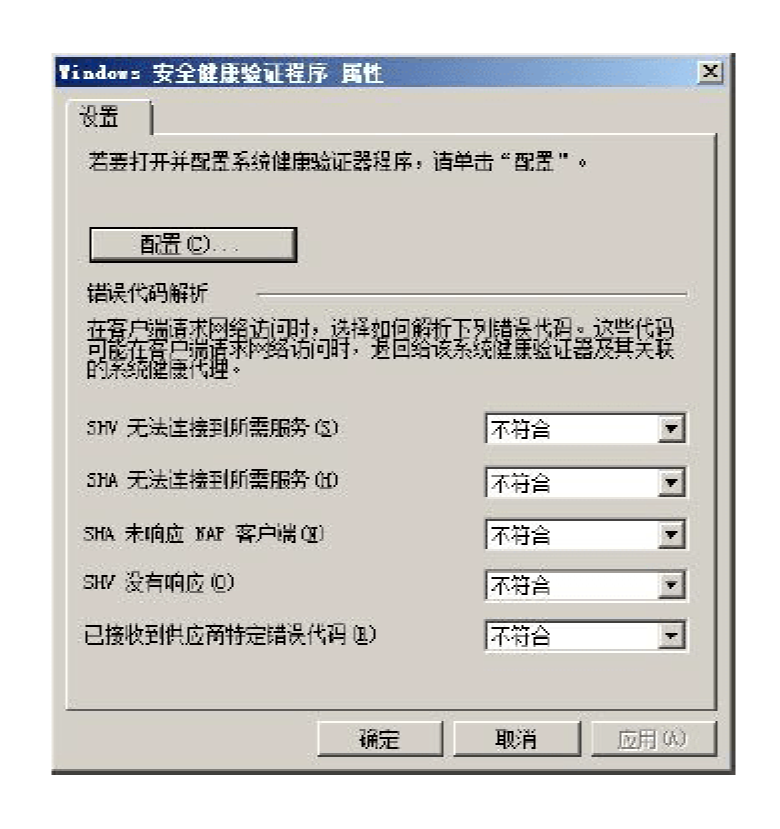


图 13-8　“Windows 安全健康验证程序 属性”对话框

在该对话框中，可以配置 NPS 解析各种错误代码。单击“配置”按钮，可以配置 Windows 安全健康验证 SHV 的健康要求，显示如图 13-9 所示的“Windows 安全健康验证程序”对话框。用户可以为 NAP 客户端选择健康要求，在 Windows Vista(在 Windows Vista 选项卡)和 Windows XP SP3(在 Windows XP 选项卡)中的 Windows 安全中心，会监视这些内嵌的 Windows 服务。

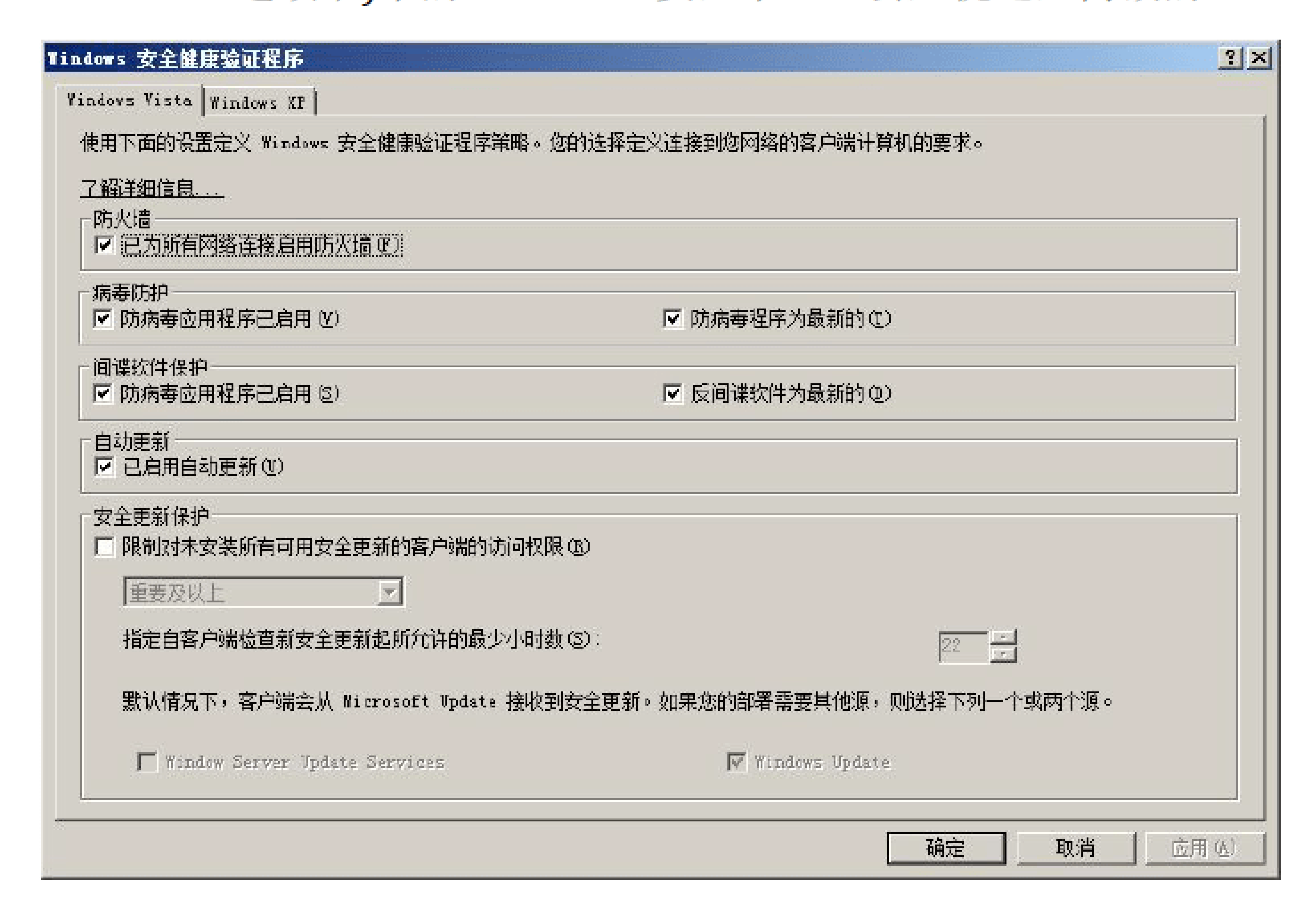


图 13-9　“Windows 安全健康验证程序”对话框

■　更新服务器组

更新服务器组是在 VPN 和 DHCP 强制方式下，不符合的 NAP 客户端和不支持 NAP 的客户端可以访问的服务器列表。对于不符合的 NAP 客户端或不支持 NAP 的客户端拥有单独的组，或者对于

不同的 NAP 强制方式拥有单独的组。

为了创建新的更新服务器组，在“网络策略服务器”控制台中，展开“网络访问保护”节点，右击“更新服务器组”并在弹出的快捷菜单中选择“新建”命令。在出现的“新建更新服务器组”对话框中，可以通过 DNS 名称、IPv4 地址或 IPv6 地址指定更新服务器，如图 13-10 所示。

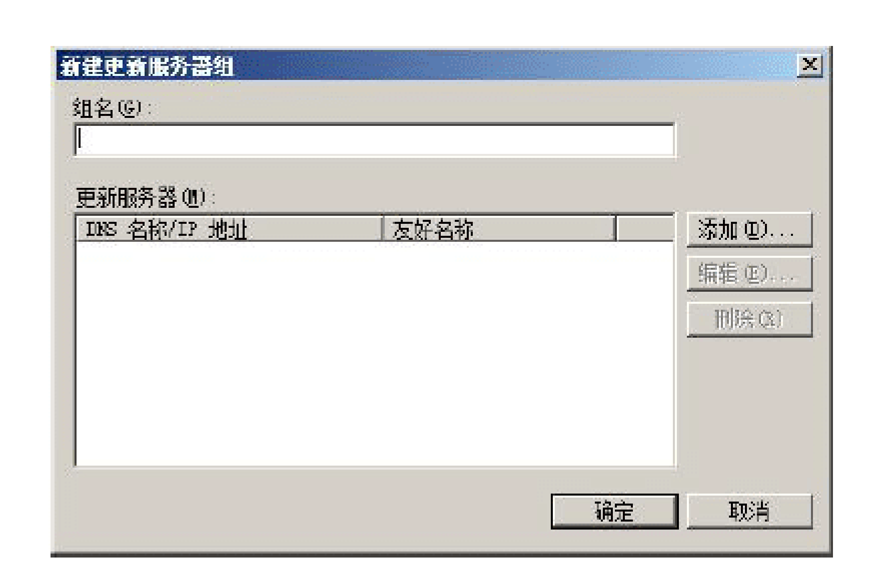


图 13-10 “新建更新服务器组”对话框

(4) 网络策略

网络策略可以指定已经被授权连接到网络的用户，以及通过无法连接到网络的环境。对于每一条规则，都包含访问权限(允许或拒绝访问)、条件、约束和网络策略设置。如果连接被授权，网络策略约束和设置可以指定一组连接约束。对于 NAP，网络策略为不符合的 NAP 客户端或未启动 NAP 的客户端指定强制行为，为健康要求指定检查条件：

- NAP 的访问权限设置。无论 NAP 健康验证是否对认证和授权的连接尝试起作用，都可以选择“授予访问权限”来保证连接请求被健康验证程序处理。连接尝试被授权，但是不符合的 NAP 客户端或不支持 NAP 的客户端仍受到限制。如果选择“拒绝访问”，连接尝试将会被拒绝，并且不会执行健康验证。用户可以创建网络策略来明确地拒绝访问，但是这些网络策略不需要 NAP 设置，因为没有必要验证不允许访问的计算机的系统健康。
- NAP 的网络策略条件。NAP 允许将如下条件添加到 NPS 网络策略中。
  - 健康策略：指定之前配置的健康策略。
  - 支持 NAP 的计算机：指定客户端是否启用 NAP。
  - 策略过期：指定网络策略过期时间和不再进行评估的时间。用户可以使用该条件从 NAP 操作的报告模式转换到强制模式。

  这里以为 NAP 网络策略使用健康策略，和支持 NAP 的计算机的条件为例进行介绍。

  - 对于只应用于通过了所有 SHV 健康要求的符合的支持 NAP 的客户端的网络策略，设置健康策略条件，指定“客户端通过了所有 SHV 检查”选项。
  - 对于只应用于未通过所有 SHV 健康要求的不符合的 NAP 客户端的网络策略，设置健康条件，指定“客户端未能通过所有 SHV 检查”选项。
  - 对于只应用于不支持 NAP 的客户端的网络策略，设置支持 NAP 的计算机条件为“仅限不支持 NAP 的计算机”。
- NAP 网络策略设置。Windows Server 2008 中的网络策略拥有一系列的 NAP 强制网络策略设置，如图 13-11 所示。对于 NAP 强制设置，可以指定如下选项。
  - 允许完全网络访问：指定连接尝试可以不受限制地访问网络。该选项适用于符合的 NAP 客户端的网络策略。
  - 允许在有限时间内对网络执行完全访问：指定连接尝试可以无限制地访问网络，不符合的 NAP 客户端计算机的用户会收到一个通知消息，通知其必须在配置的日期和时间之内变为符合的。该方式也称延期强制模式。
  - 允许受限访问：指定连接尝试网络访问受限。不符合的 NAP 客户端计算机的用户会收到“该计算机不符合网络要求”的消息。该选项适用于不符合的 NAP 客户端或不支持 NAP 的客户端的网络策略。该方式也称强制模式。

- 启用客户端计算机的自动更新功能：指定 NAP 客户端是否必须自动更新。

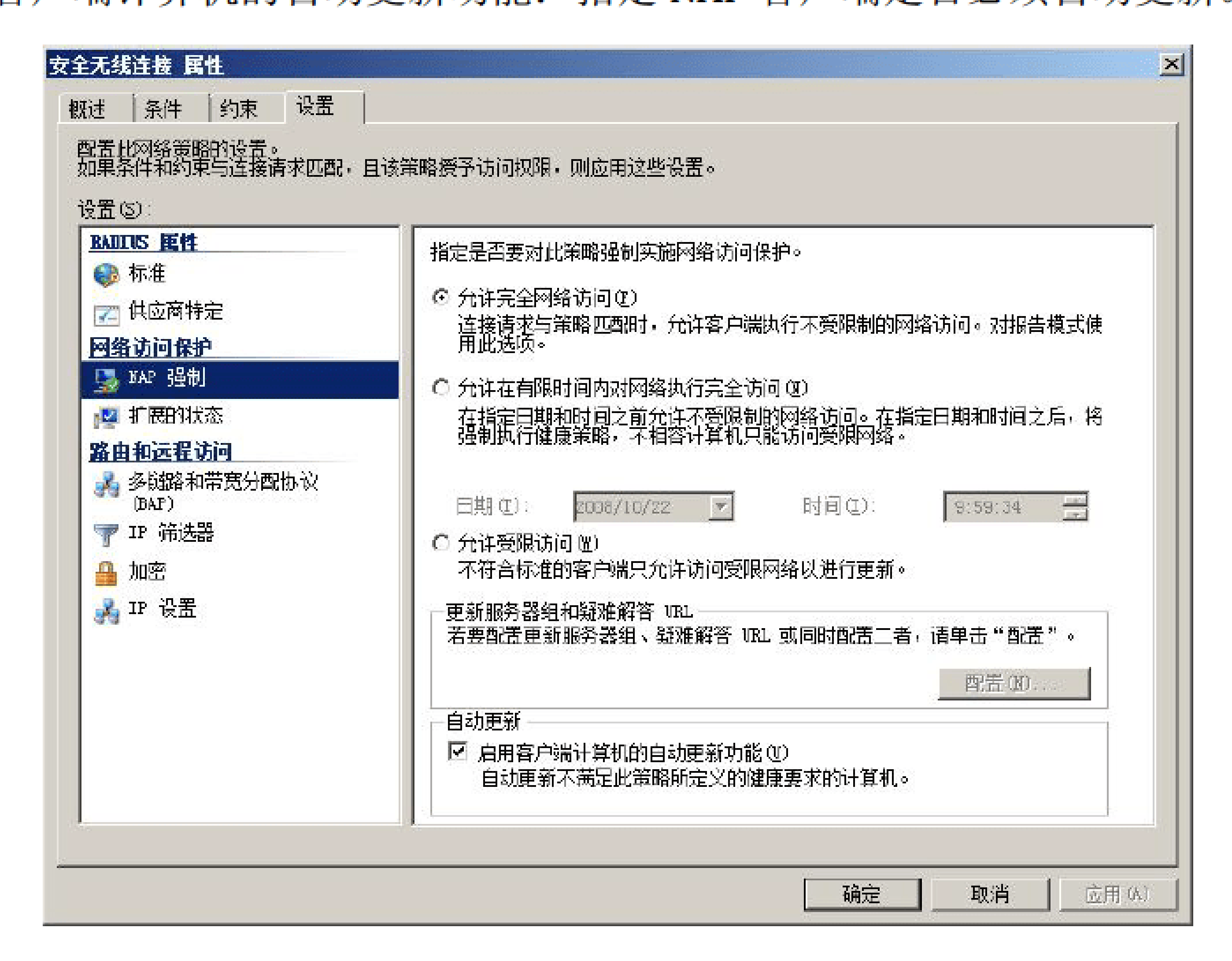


图 13-11　NAP 强制设置

对于受限访问，单击“配置”按钮，显示如图 13-12 所示的“更新服务器和疑难解答 URL”对话框，指定更新服务器组和疑难解答 URL。

在“更新服务器组”下拉列表中，选择之前配置的更新服务器组，或者单击“新建组”按钮，弹出如图 13-13 所示的“新建更新服务器组”对话框，创建新的更新服务器组。在“疑难解答 URL”文本框中，输入更新服务器的 Web 页面的 URL。该 URL 当用户单击“网络访问保护”对话框中的“详细信息”时是活动的。

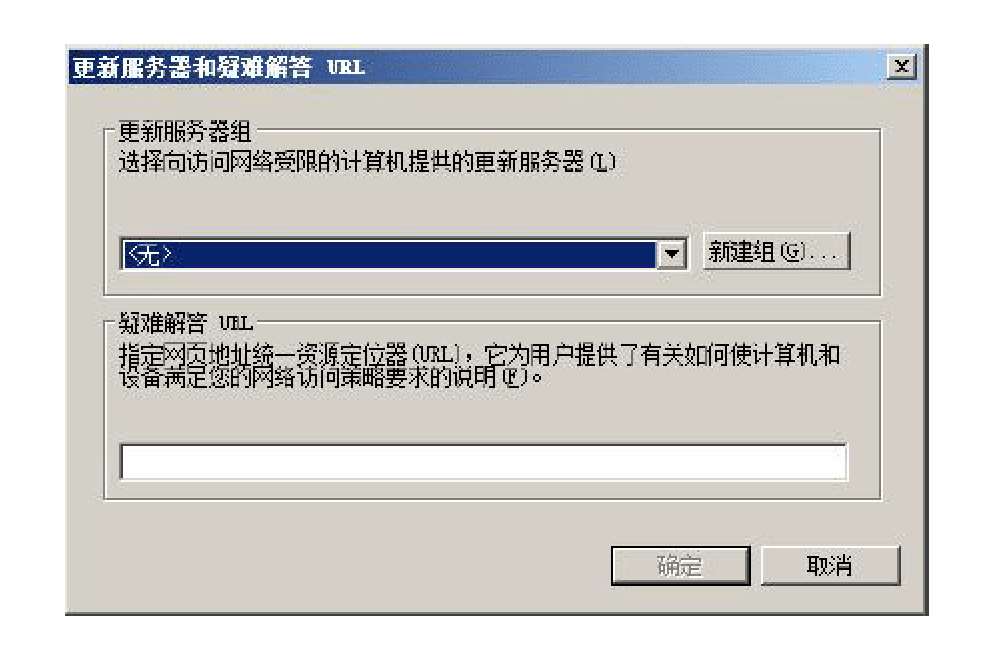


图 13-12　“更新服务器和疑难解答 URL”对话框

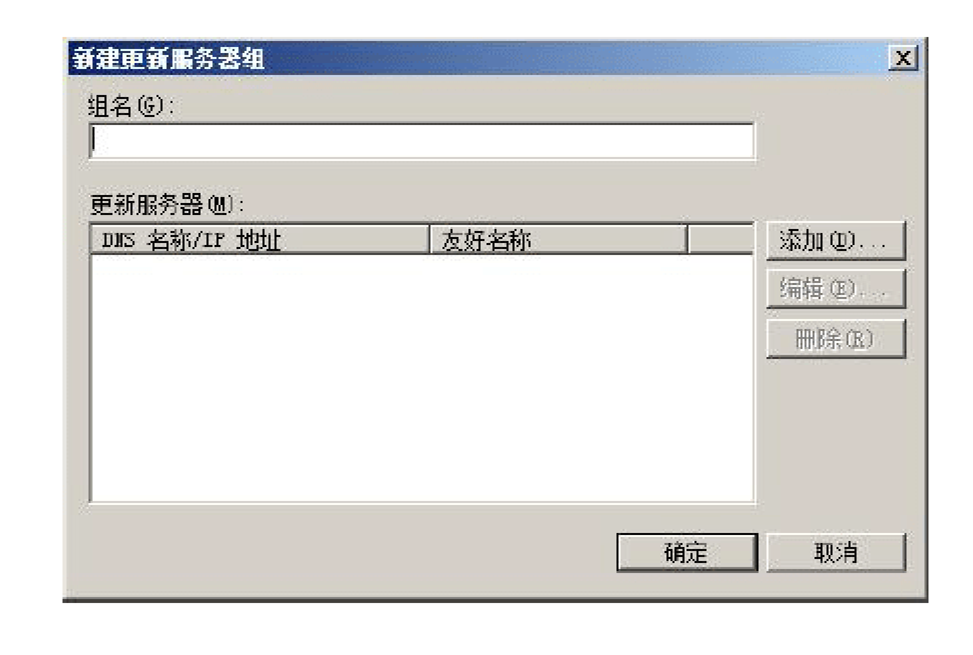


图 13-13　“新建更新服务器组”对话框

在 Web 页面中，可以确定如何更新计算机使之变为符合的或执行网络访问的疑难解答。在 netsh nap client show state 命令显示中该 URL 也是可见的。

(5)　配置 NAP 向导

通过“配置 NAP 向导”可以简单地完成 NAP 健康要求策略的初始配置。

① 依次选择“开始”→“管理工具”→“网络策略服务器”命令，显示如图 13-14 所示的“网络策略服务器”窗口。在右侧下拉列表中，选择“网络访问保护(NAP)”选项。



图 13-14 “网络策略服务器”窗口

② 单击“配置 NAP”按钮，显示如图 13-15 所示的“选择与 NAP 一起使用的网络连接方法”界面。根据需要，在下拉列表中选择网络连接方式(NAP 强制方式)，系统会自动为 NAP 健康要求策略创建一个名称，也可根据需要进行修改。这里选择“带有健康注册机构(HRA)的 IPSec”网络连接方法。

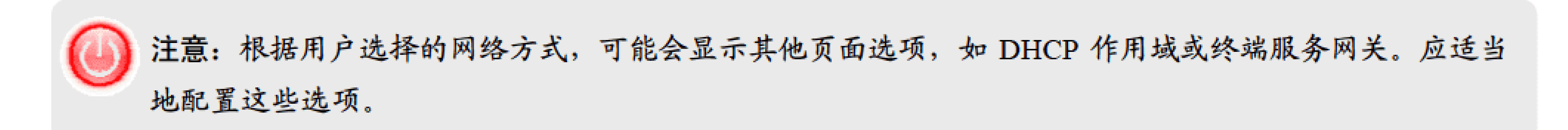
③ 单击“下一步”按钮，显示如图 13-16 所示的“指定 NAP 强制服务器运行 HRA”界面，根据 NAP 强制点添加、编辑或移除 RADIUS 客户端。配置 NAP 向导只是允许用户添加 RADIUS 客户端来代替在 RADIUS 客户端节点中手动添加。



图 13-15 “选择与 NAP 一起使用的网络连接方法”界面



图 13-16 “指定 NAP 强制服务器运行 HRA”界面


注意：根据用户选择的网络方式，可能会显示其他页面选项，如 DHCP 作用域或终端服务网关。应适当地配置这些选项。

④ 单击“下一步”按钮，显示如图 13-17 所示的“配置用户组和计算机组”界面。单击“添加计算

机”按钮，添加计算机组或用户组来指定向导创建的网络策略，可以只应用于特定计算机组的计算机账户，或只应用于特定用户组的用户账户。

⑤ 单击“下一步”按钮，显示如图 13-18 所示的“定义 NAP 健康策略”界面。根据需要配置用户想要强制的 SHV、自动更新行为和对于不支持 NAP 的计算机的行为。

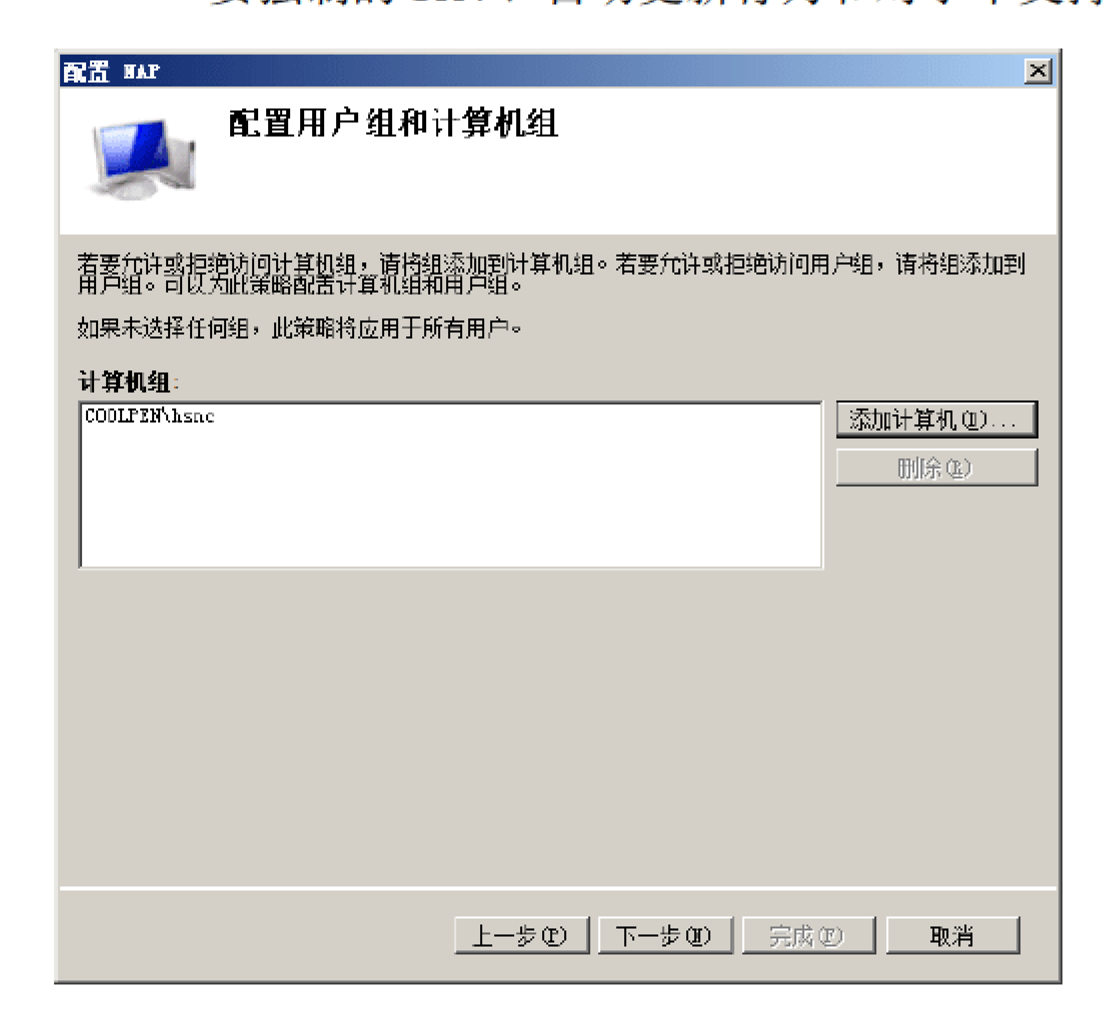


图 13-17　“配置用户组和计算机组”对话框

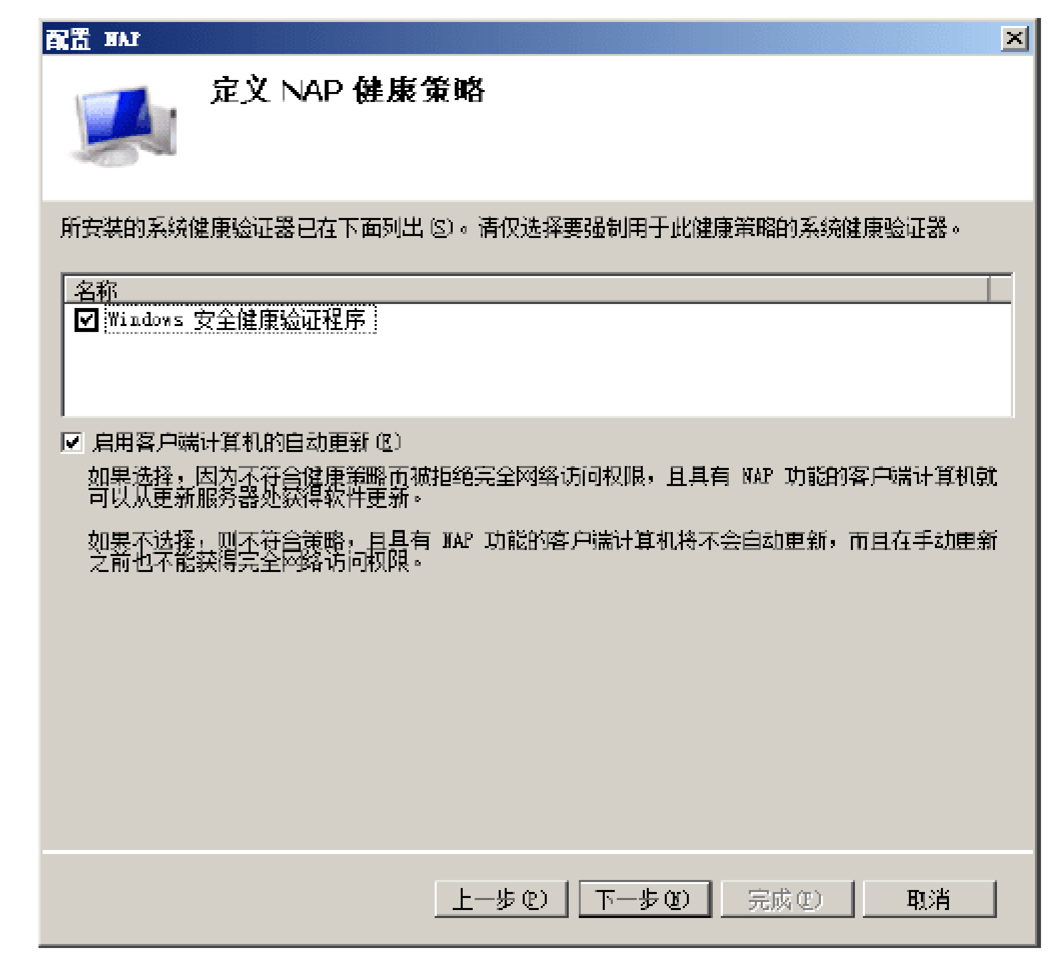


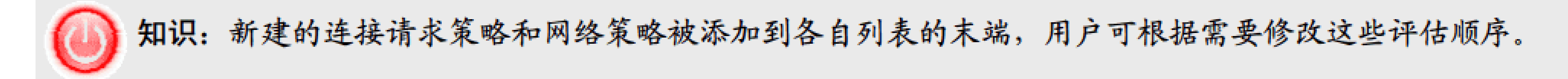
图 13-18　“定义 NAP 健康策略”界面

⑥ 单击“下一步”按钮，显示如图 13-19 所示的“正在完成 NAP 增强策略和 RADIUS 客户端配置”界面。“配置 NAP 向导”的结果如图中所示。



图 13-19　“正在完成 NAP 增强策略和 RADIUS 客户端配置”界面

⑦ 单击“完成”按钮，完成 NAP 的配置。在“网络策略服务器”窗口左侧控制台中，展开“策略”→“连接请求策略”节点，新添加的策略即可显示在右侧栏中，如图 13-20 所示。



知识：新建的连接请求策略和网络策略被添加到各自列表的末端，用户可根据需要修改这些评估顺序。

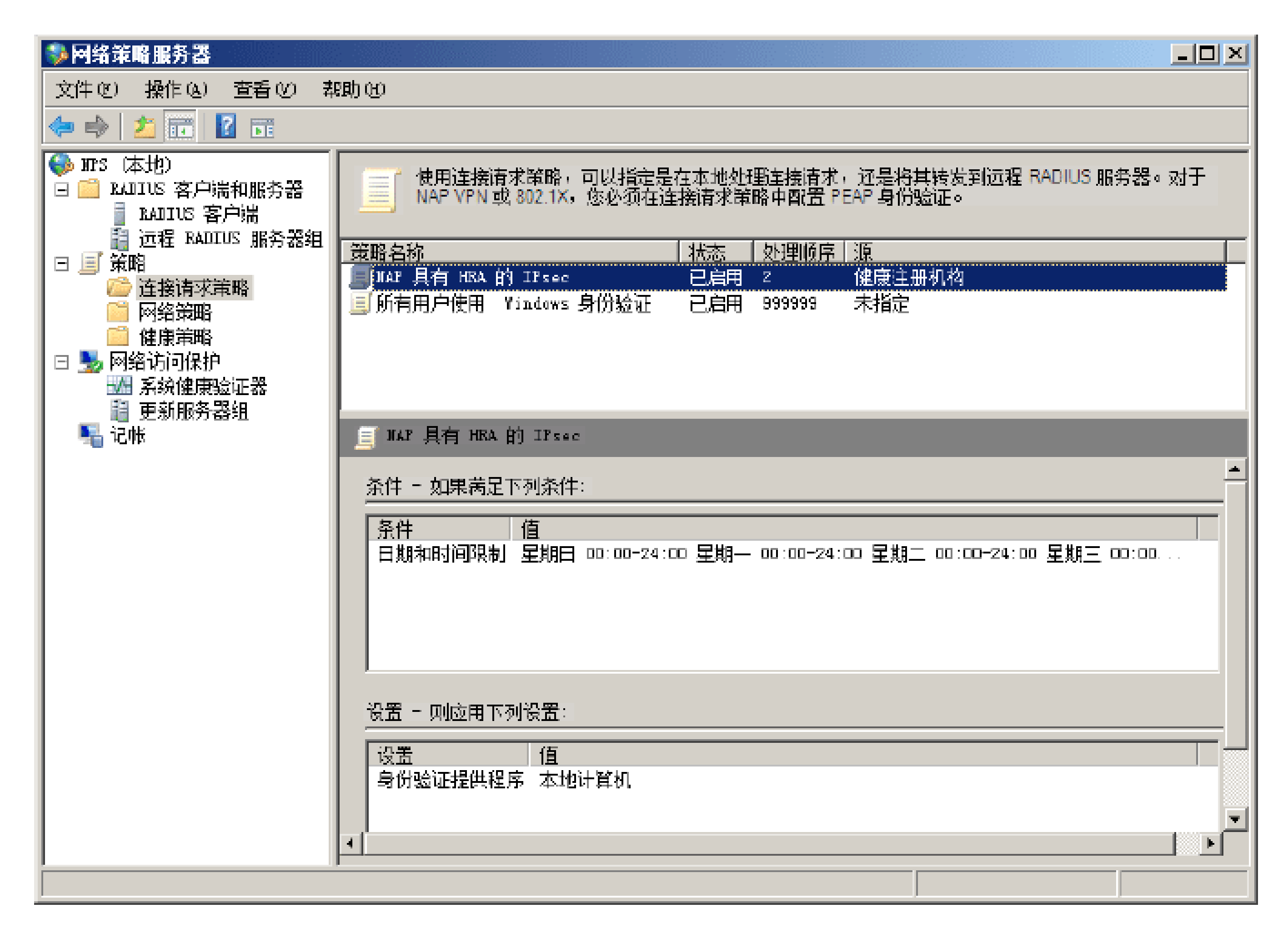


图 13-20　查看连接请求策略

2. NAP 健康评估工作过程

在 NAP 健康策略服务器上的 NPS 服务通过如下过程来执行健康评估。

① 当 NAP 健康策略服务器上的 NPS 服务，从 NAP 强制点收到 RADIUS 访问请求消息时，首先确定该消息是否来自相应的配置好的 RADIUS 客户端的地址。如果答案是否，则 NPS 服务丢弃该消息。NAP 健康策略服务器处理来自未配置的 RADIUS 客户端的 RADIUS 消息。

② NPS 服务比较访问请求消息和配置的连接请求消息。对于 NAP，访问请求消息需要与指定 NPS 服务执行认证和授权的连接请求策略匹配。

③ NPS 服务评估访问请求消息中的健康信息，该信息包含在 SSoH 中。NPS 将每个 SoH 发送给相应的 SHV 进行评估。评估结果包含在 SHV 的 SoHR 中。

④ NPS 服务依靠网络策略评估访问请求消息和 SoHR。SoHR 如同 NAP 网络策略的健康策略条件。NPS 服务应用最好的匹配网络策略于访问请求消息。最好的匹配网络策略是首先与指定源匹配的网络策略，或者首先与未指定源匹配的网络策略。

⑤ 根据最好匹配策略和网络策略的网络访问保护设置，NPS 服务创建健康响应的系统状态(SSoHR)，包括 SHV 的 SoHR 和如下指示：

- NAP 客户端可以不受限访问。
- NAP 客户端访问受限。这种情况下，SSoHR 也指示客户端是否应该自动尝试更新不符合的健康状态。

⑥ NPS 服务发送包含 SSoHR 的 RADIUS 访问接受消息到 NAP 强制点。如果客户端访问受限，访问接收消息也可以包含 RADIUS 属性，指定 NAP 客户端访问如何受限。

⑦ NAP 强制点发送 SSoHR 到 NAP 客户端。

第 14 章　NAP 应用技术

网络策略服务器可以为多种网络服务提供健康策略评估，常用强制方式有 IPSec 策略强制、802.1X 端口的有线和无线网络访问控制、VPN 远程访问限制和 DHCP 地址租约和续订限制。每一种 NAP 强制方法都有其适用场合和范围。通过组合强制方法，可以消除 NAP 部署中的大部分缺点。但是，同时部署多种 NAP 强制方法可能会使 NAP 难以管理。

关键词

- 配置 IPSec 强制
- 配置 802.1X 强制
- 配置 VPN 强制
- 配置 DHCP 强制

14.1 配置 IPSec 强制

IPSec 强制的配置主要包括如下内容：配置活动目录、配置 PKI、配置 HRA、配置 NAP 健康策略服务器、配置边界网络中的更新服务器、配置 NAP 客户端与配置和应用 IPSec 策略。

14.1.1 配置 PKI

为 IPSec 强制配置基于 Windows 的 PKI，需要完成如下工作：

- 添加根 CA(根据需要)。
- 在发布 CA 级别创建 NAP CA。
- 验证 NAP CA 属性(企业 CA)。
- 为健康证书创建证书模板(企业 CA)。
- 配置 NAP CA 允许非默认的生命周期(企业 CA)。
- 配置健康证书模板的自动注册(企业 CA)。
- 为健康证书公布证书模板(企业 CA)。
- 配置证书的自动注册。

1. 添加根 CA

如果用户没有基于 Windows 的 PKI，则必须在安全网络中的计算机上创建根 CA，根据企业需要和安全策略创建中间一级的 CA。

2. 在发布 CA 级别创建 NAP CA

为了在运行 Windows Server 2008 的计算机上添加 NAP CA，可以使用“服务器管理器”，安装活动目录证书服务角色。对于 NAP CA，不需要证书颁发机构 Web 自动注册、联机应答，或网络设备自动注册服务角色。在安装活动目录证书服务角色的过程中，如果 NAP 客户端没有使用 HRA 的 DNS 发现，保证 NAP CA 计算机作为证书层级的发布 CA 中的从属、独立的 CA。此时，保证 NAP CA 计算机是从属的企业 CA。

如果添加 NAP CA 到运行 Windows Server 2003 的计算机上，可以在“控制面板”的“添加或删除程序”窗口中，使用“Windows 组件向导”安装证书服务组件。在安装证书服务组件过程中，保证 NAP CA 计算机作为证书层级的发布 CA 中的从属的 CA。

3. 验证 NAP CA 的属性

必须验证 NAP CA 不需要管理员批准要求的证书，具体操作步骤如下。

① 依次单击“开始”→“管理工具”→Certification Authority 命令，打开 Certification Authority 窗口，右击 NAP CA 的名称并在弹出的快捷菜单中选择“属性”命令，显示如图 14-1 所示的证书属性对话框。

② 切换到“策略模块”选项卡，单击“属性”按钮，显示如图 14-2 所示的“属性”对话框。在“请求处理”选项卡中，选择“如果可以的话，按照证书模板中的设置。否则，将自动颁发证书。”单选按钮。

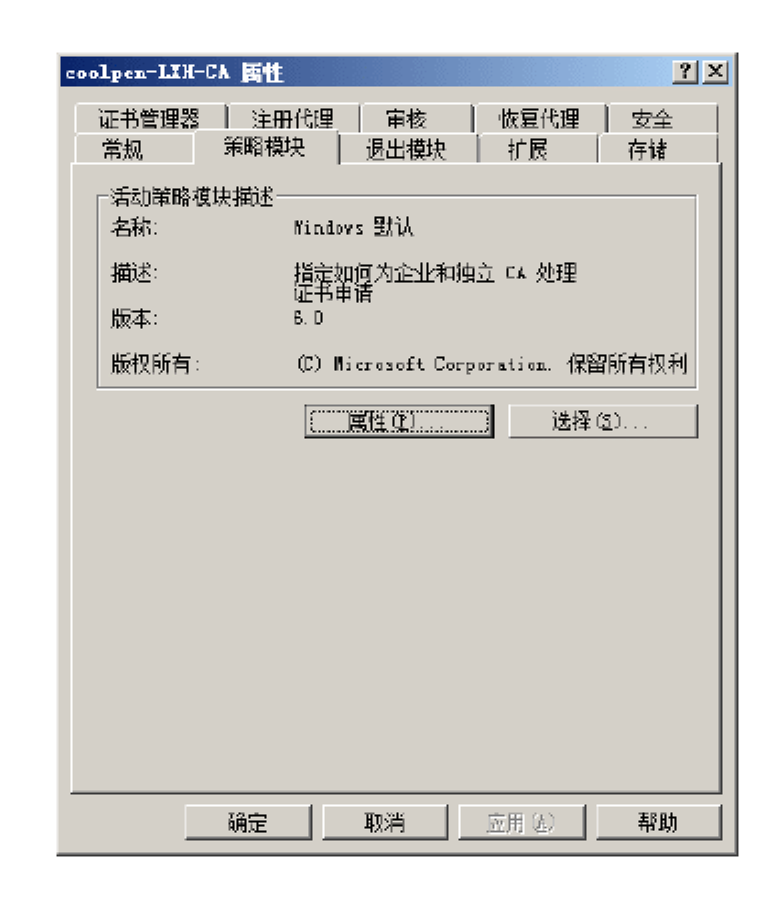



图 14-1　证书属性对话框

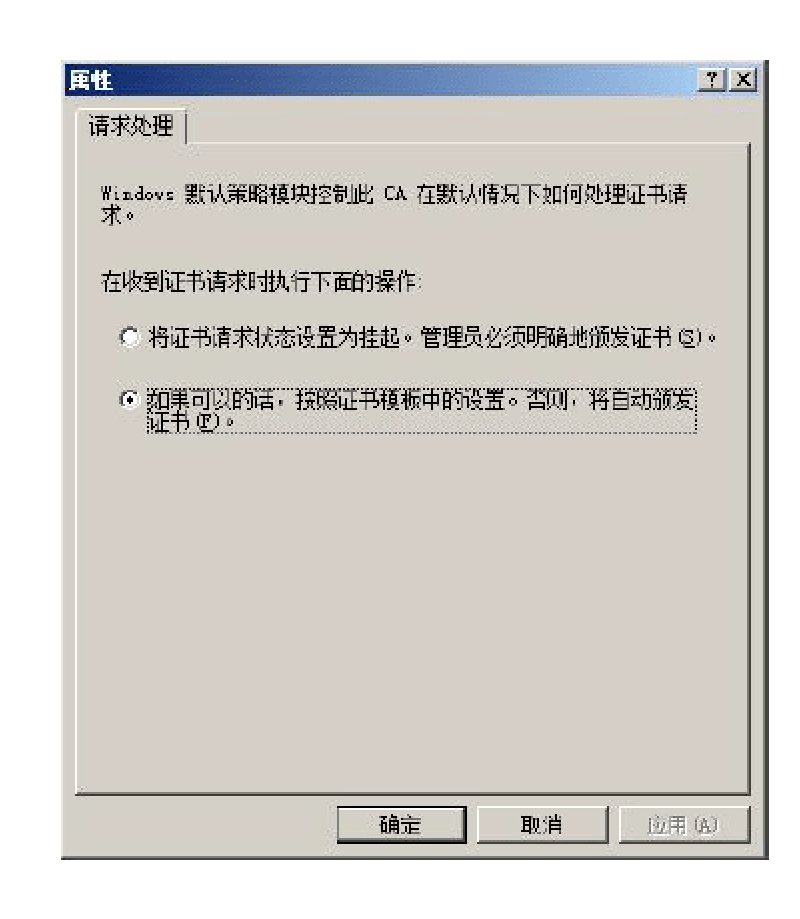


图 14-2　“属性”对话框

③　连续单击“确定”按钮，保存设置。

4. 为健康证书创建证书模板

对于基于 Windows Server 2003 的 NAP CA，必须手动创建系统健康身份验证证书模板，从而保证 IPSec 安全组的成员可以自动注册长生命周期的健康证书。对于基于 Windows Server 2008 的 NAP CA，系统中已经包括了系统健康身份验证证书模板，但是，必须确保系统健康身份验证证书模板拥有适当的自动注册的权限。

①　单击“开始”→“运行”命令，在“打开”文本框中输入“certtmpl.msc”，并按 Enter 键运行，显示如图 14-3 所示的“证书模板控制台”窗口。

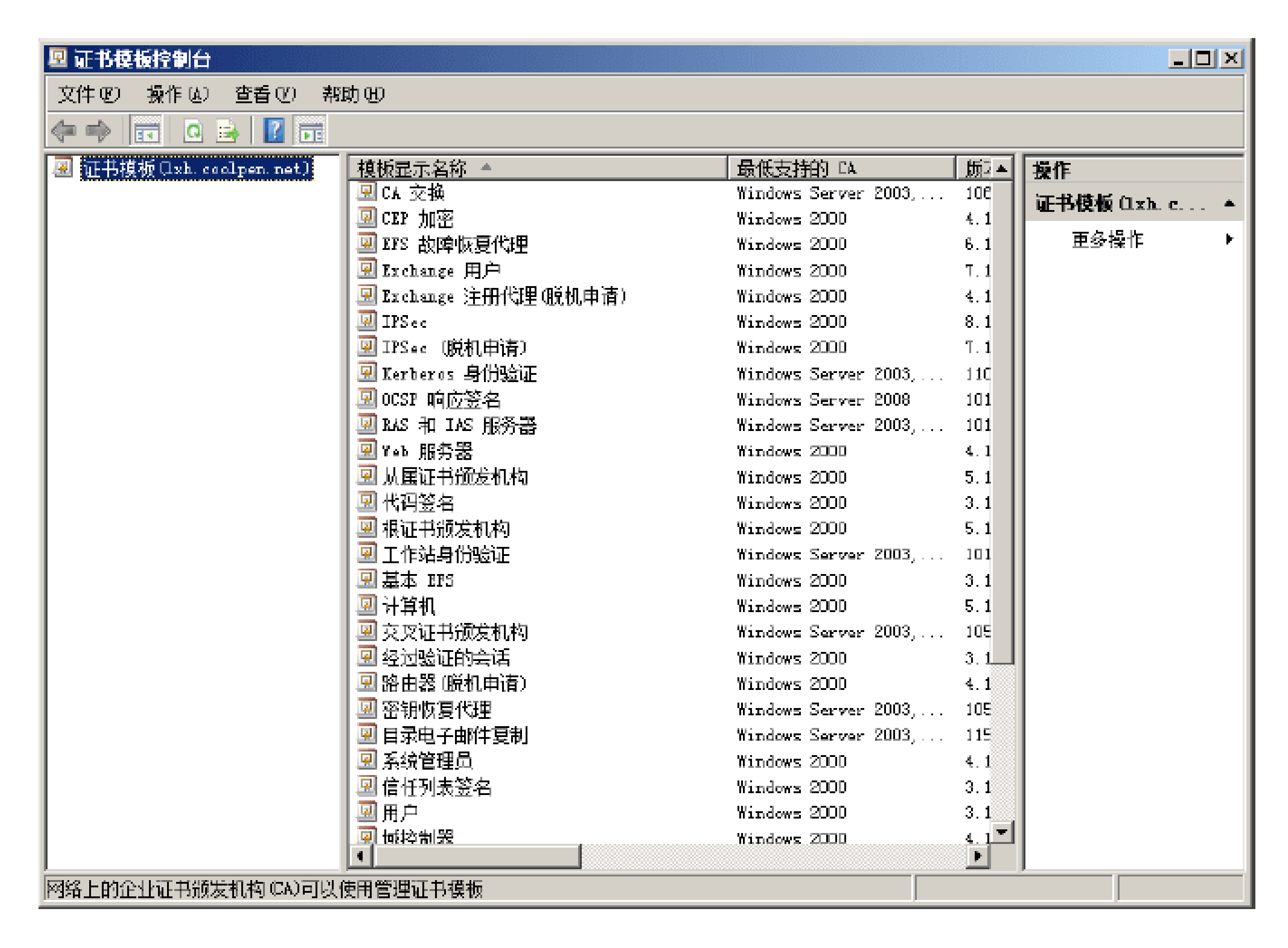


图 14-3　“证书模板控制台”窗口

②　右击“工作站身份验证”并在弹出的快捷菜单中选择“复制模板”选项，显示如图 14-4 所示的“新模板的属性”对话框。在“模板显示名称”文本框中，输入“系统健康身份验证”。选中“在 Active Directory 中发布证书”复选框，使该证书在域环境中颁发。

③ 切换到“扩展”选项卡，在“这个模板中包括的扩展”列表框中，选择“应用程序策略”选项。单击“编辑”按钮，显示如图 14-5 所示的“编辑应用程序策略扩展”对话框。

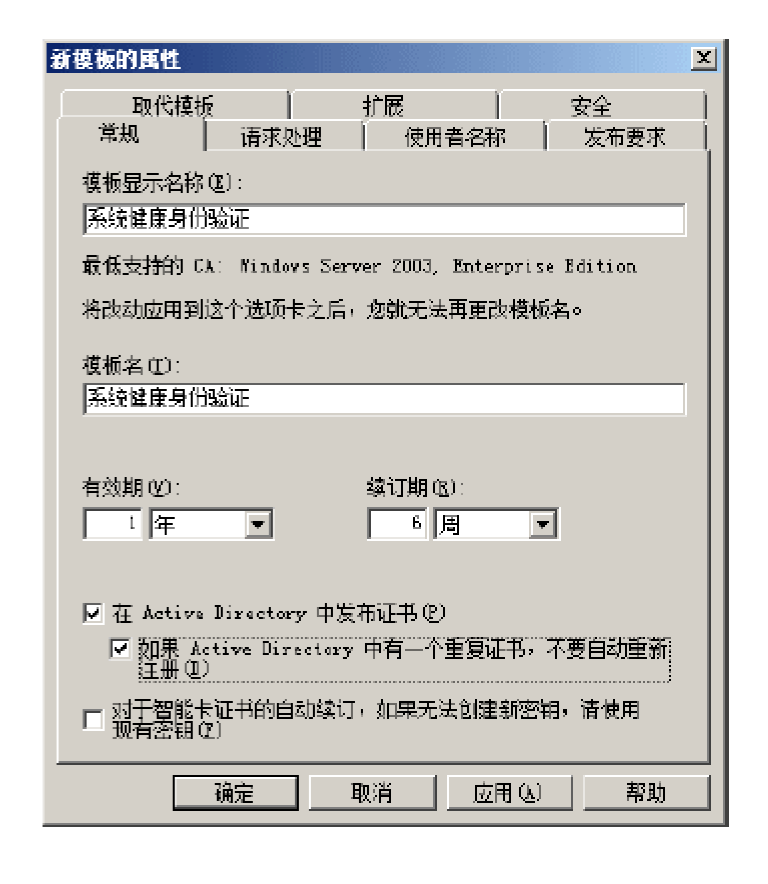



图 14-4 “新模板的属性”对话框

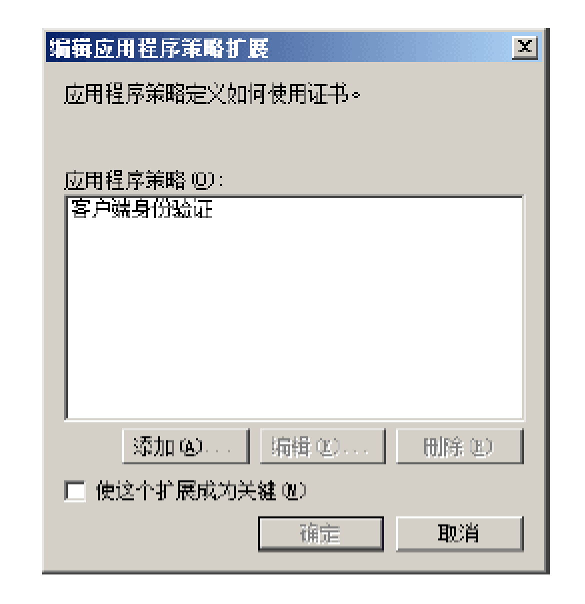


图 14-5 “编辑应用程序策略扩展”对话框

④ 单击“添加”按钮 ，显示如图 14-6 所示的“添加应用程序策略”对话框。在“应用程序策略”列表框中，选择“系统健康身份验证”选项。

⑤ 连续单击“确定”按钮，返回“新模板的属性”对话框，切换到如图 14-7 所示的“安全”选项卡。

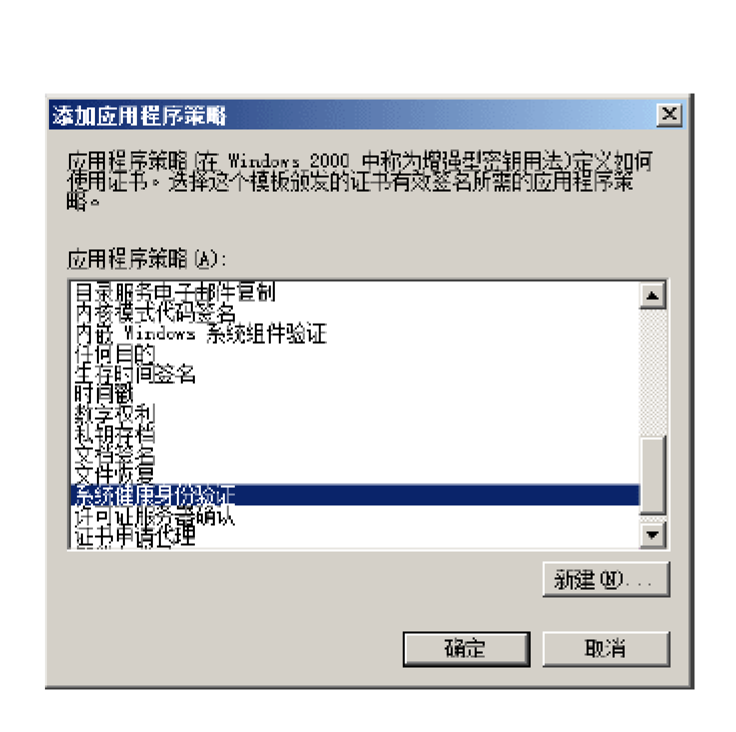


图 14-6 “添加应用程序策略”对话框

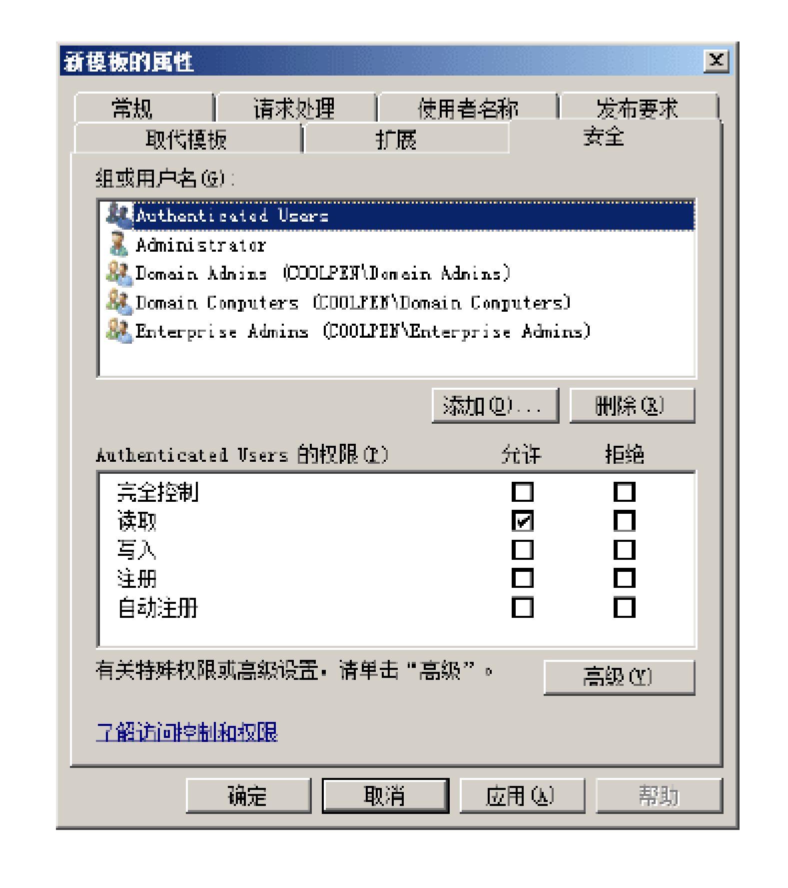


图 14-7 “安全”选项卡

⑥ 单击“添加”按钮，显示如图 14-8 所示的“选择用户、计算机或组”对话框，输入 IPSec NAP 安全组的名称，单击“检查名称”按钮，检查输入的组名是否正确。

⑦ 单击“确定”按钮，在“安全”选项卡中，选择 IPSec NAP 安全组的名称，在“IPSec 的权限”列表框中选中“注册”和“自动注册”对应的“允许”复选框，如图 14-9 所示。

⑧ 单击“确定”按钮，保存设置。此时，新模板即可添加到模板控制台中，如图 14-10 所示。

5. 发布新的健康证书模板

① 在根 CA 计算机上，运行“证书颁发机构”管理单元，如图 14-11 所示。

② 右击“证书模板”，在弹出的快捷菜单中选择“新建”→“要颁发的证书模板”命令，显示如

图 14-12 所示的“启用证书模板”对话框。



图 14-8　“选择用户、计算机或组”对话框

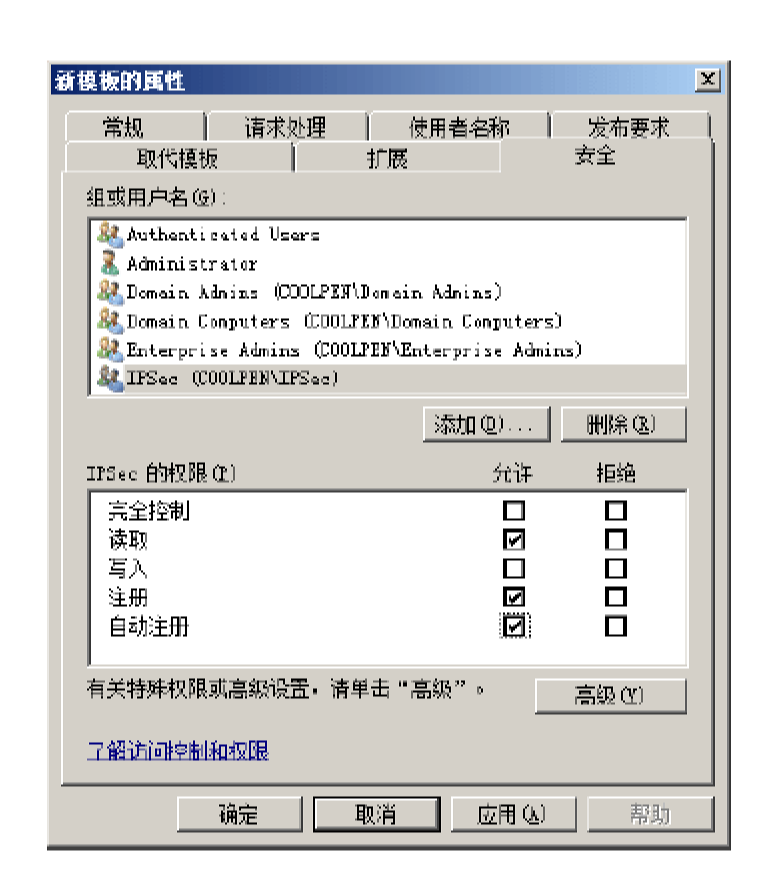


图 14-9　赋予用户相应的权限

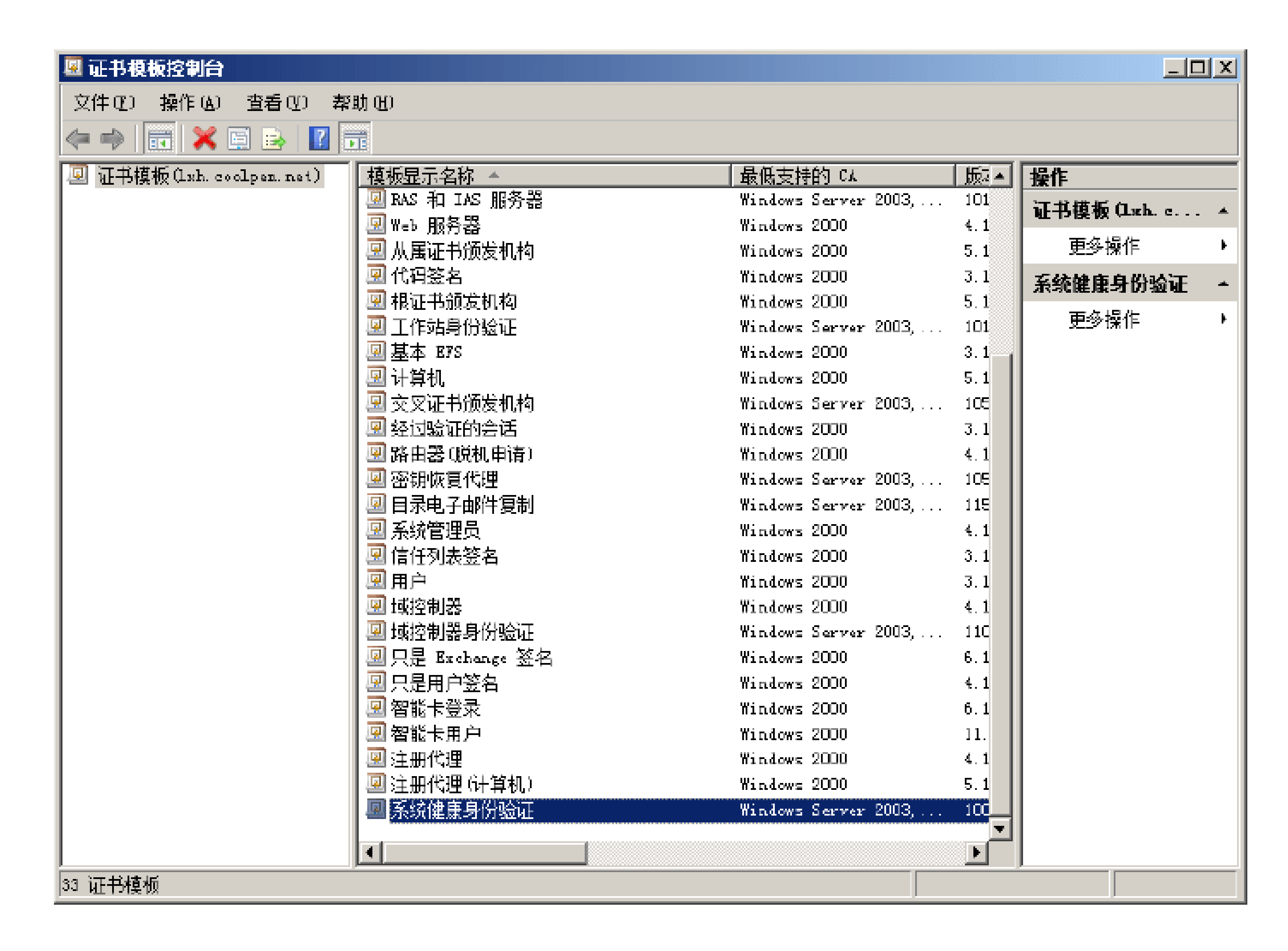


图 14-10　成功添加模板

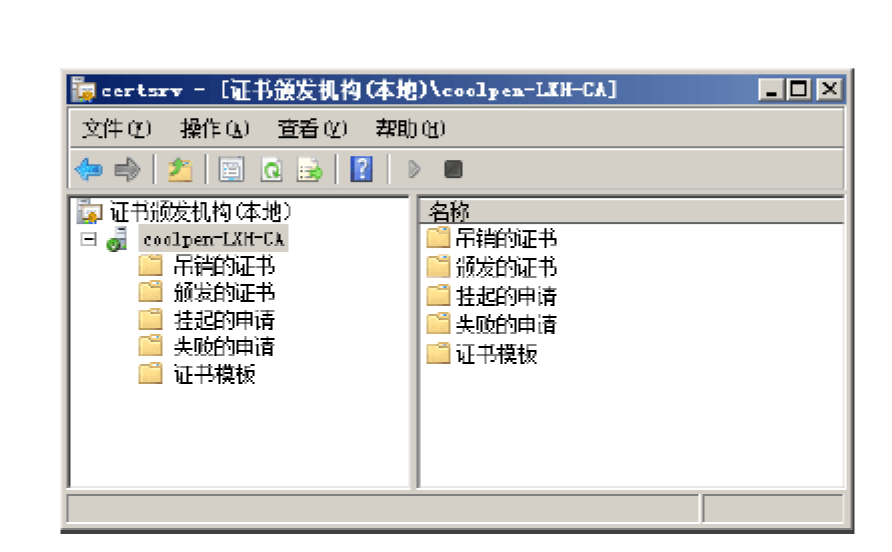


图 14-11　“证书颁发机构”窗口

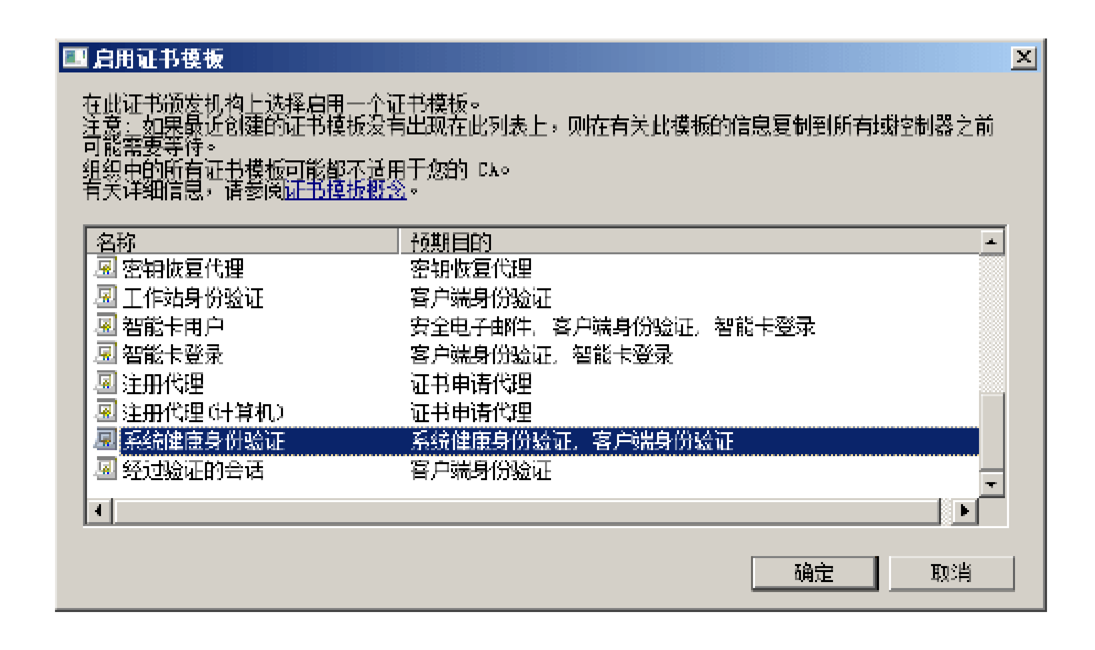


图 14-12　“启用证书模板”对话框

③ 选中“系统健康身份验证”，单击“确定”按钮，即可颁发该模板，如图 14-13 所示。



图 14-13　成功颁发新的模板

6. 配置 NAP CA 允许非默认的生命周期

企业 NAP CA 必须配置为允许非默认的生命周期。否则，符合的 NAP 客户端将被发布健康证书模板指定的生命周期的健康证书，而不是 HRA 配置中指定的短生命周期。

配置企业 NAP CA 允许非默认的生命周期的具体操作步骤如下。

① 在企业 NAP CA 计算机的命令行中，运行 certutil.exe –setreg policy\EditFlags +EDITF_ATTRIBUTEENDDATE 命令，结果如图 14-14 所示。

```
管理员: 命令提示符
C:\Users\Administrator>certutil.exe  -setreg policy\EditFlags +EDITF_ATTRIBUTEEN
DDATE
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\coolpen-LXH-CA\PolicyMod
ules\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:

旧值:
  EditFlags REG_DWORD = 11014e (1114446)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)

新值:
  EditFlags REG_DWORD = 11016e (1114478)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_ATTRIBUTEENDDATE -- 20 (32)
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -setreg 命令成功完成。
CertSvc 服务可能需要重新启动，以使更改生效。

C:\Users\Administrator>
C:\Users\Administrator>
```

图 14-14　配置企业 NAP CA

② 运行 net stop certsvc 和 net start certsvc 命令，重启活动目录证书服务，如图 14-15 所示。

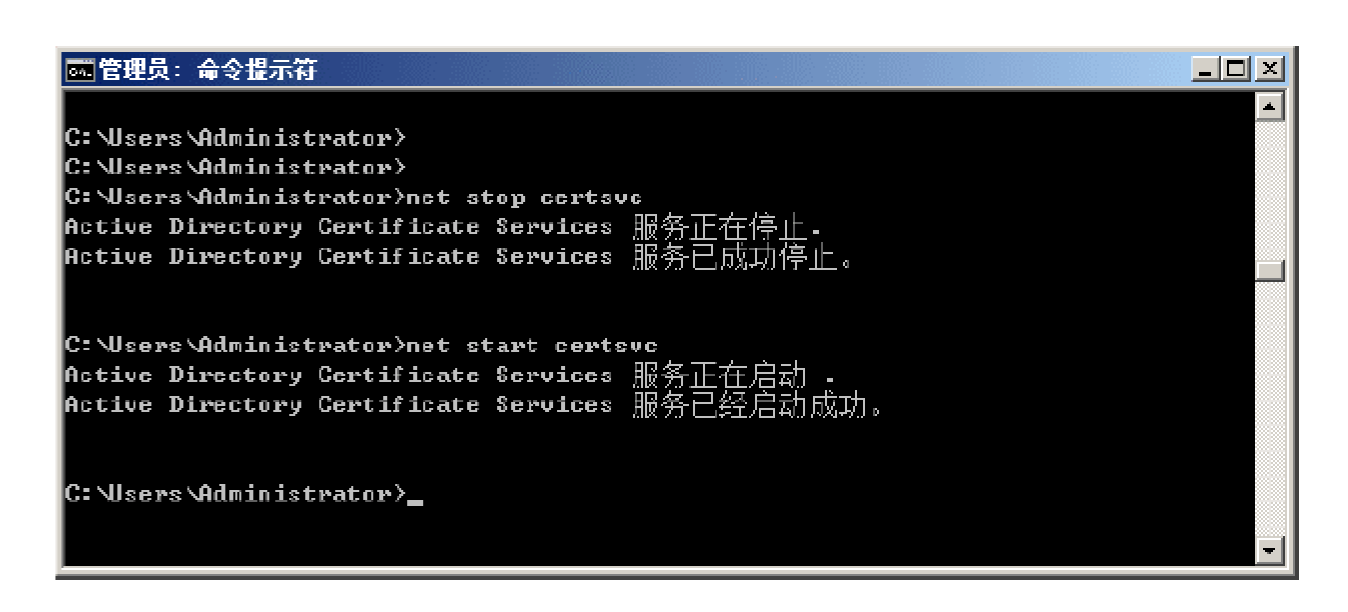


图 14-15　重启活动目录证书服务

7. 配置健康证书模板的自动注册

为了使边界计算机(IPSec NAP 安全组成员)自动获取长生命周期的健康证书，必须在活动目录中启用证书自动注册。

在“组策略管理编辑器”中，展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“公钥策略”节点。双击“证书服务客户端 - 自动注册”选项，显示如图 14-16 所示的“证书服务客户端 - 自动注册 属性”对话框。在“配置型号”下拉列表中，选择“已启用”选项，并选中“续订过期证书、更新未决证书并删除吊销的证书”和“更新使用证书模板的证书”复选框。单击“确定”按钮，保存设置。

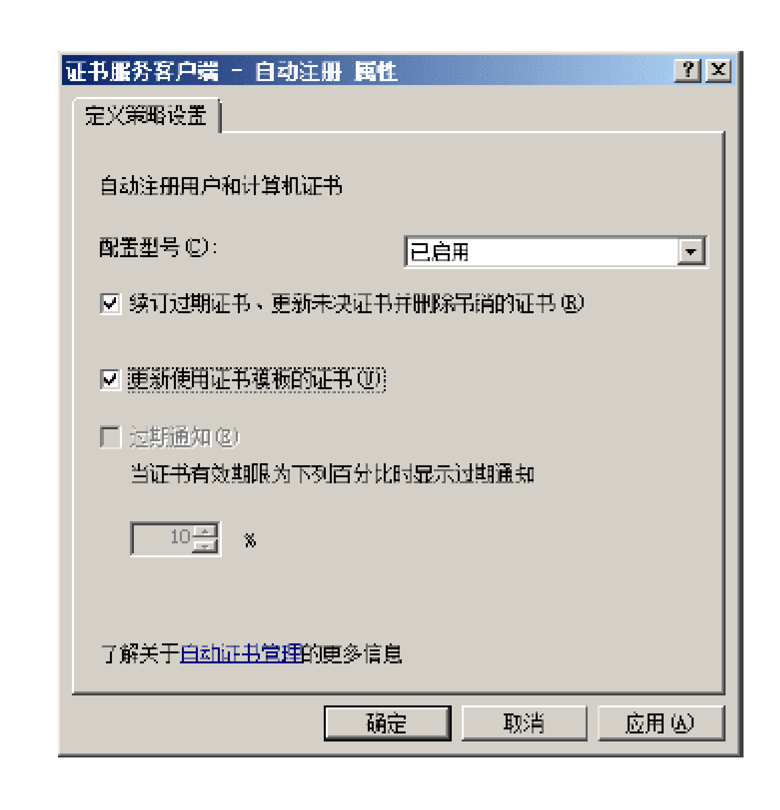


图 14-16　“证书服务客户端-自动注册 属性”对话框

14.1.2　配置 HRA

配置 HRA 主要包括添加 HRA 到 IPSec NAP 安全组、安装计算机证书、配置网络策略和访问服务角色、使用 HRA 权限配置 NAP CA、配置 HRA 的属性、为 RADIUS 代理在 HRA 上配置 NPS 服务和为 SSL 配置 IIS。

1. 添加 HRA 到 IPSec NAP 安全组

HRA 计算机账户必须是 IPSec NAP 安全组中的成员，以保证其立即拥有一个长期的健康证书，允许其与安全网络中的计算机通信。添加 HRA 计算机账户到 IPSec NAP 安全组中的步骤如下。

① 在“活动目录用户和计算机”窗口中，双击 IPSec NAP 安全组的名称，显示如图 14-17 所示的“IPSec 属性”对话框。

② 切换到“成员”选项卡，单击“添加”按钮，显示“选择用户、联系人、计算机或组”对话框。单击“对象类型”按钮，显示如图 14-18 所示的“对象类型”对话框。选中“计算机”复选框。

③ 单击“确定”按钮，返回“选择用户、联系人、计算机或组”对话框。在“输入对象名称来选择”文本框中，输入 HRA 计算机的名称，单击“检查对象”按钮，检查输入的计算机是否正确。

④ 连续单击“确定”按钮，保存设置即可。

2. 使用 HRA 权限配置 NAP CA

NAP CA 必须配置允许 HRA 组件请求证书的权限，HRA 计算机也可以被授予管理 CA 的权限，以保证其可以从 NAP CA 证书数据库中自动删除过期的证书。

① 在“证书颁发机构”管理单元，右击 NAP CA 的名称，在弹出的快捷菜单中选择“属性”命令，

打开“coolpen-LXH-CA 属性”对话框，并切换到“安全”选项卡。

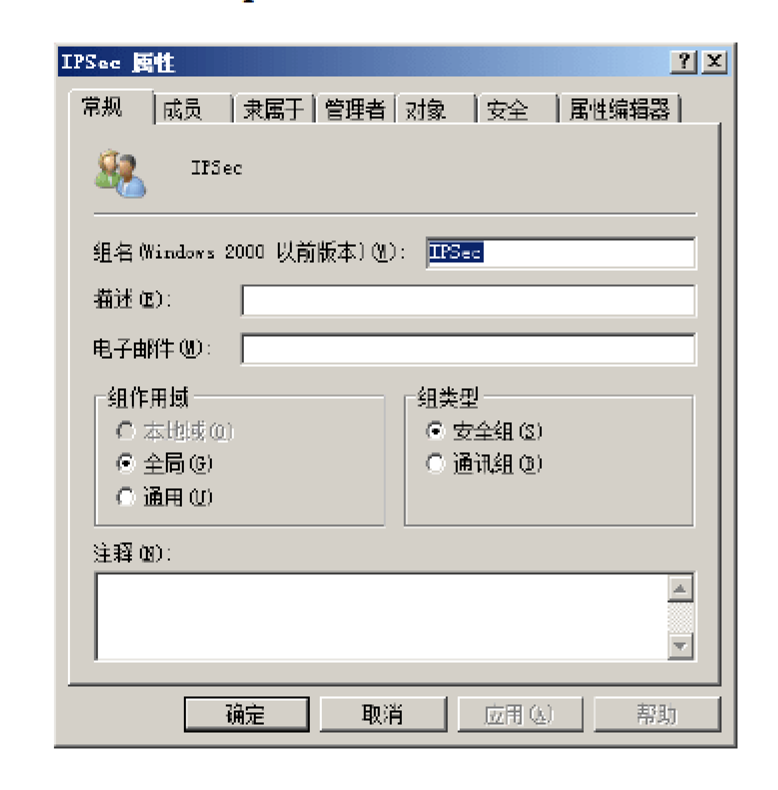


图 14-17 “IPSec 属性”对话框

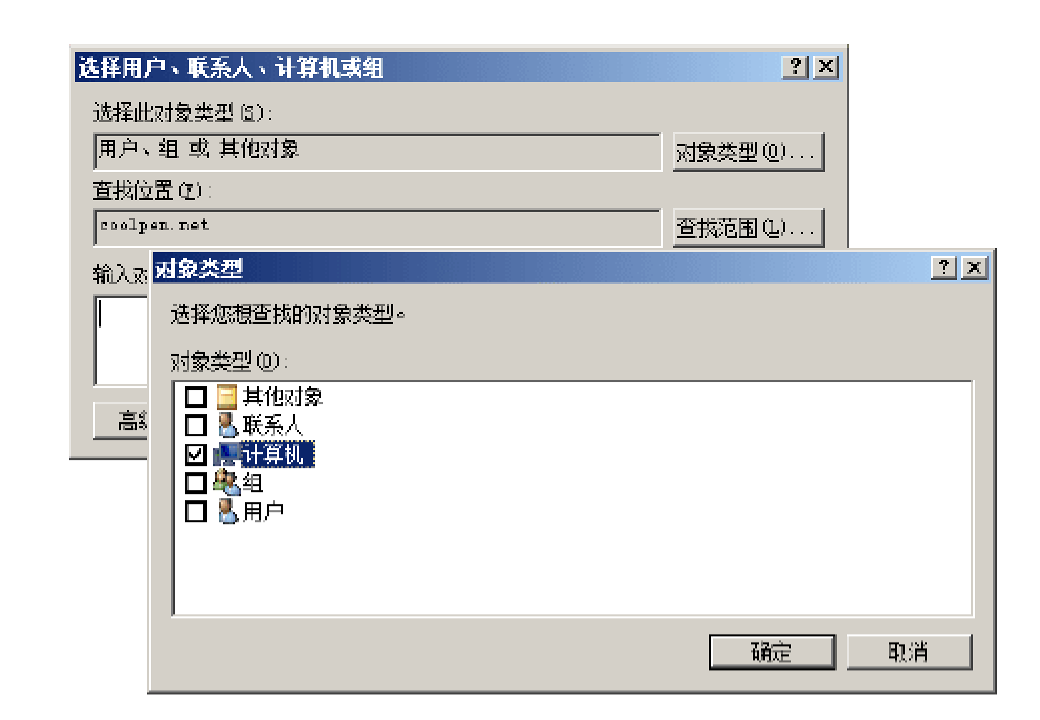


图 14-18 “对象类型”对话框

② 单击“添加”按钮，打开“选择用户、计算机或组”对话框。单击“对象类型”按钮，显示如图 14-19 所示的“对象类型”对话框。选中“计算机”复选框。

③ 单击“确定”按钮，返回“选择用户、计算机或组”对话框。在“输入对象名称来选择”文本框中，输入 HRA 计算机的名称，单击“检查对象”按钮，检查输入的计算机名是否正确。

④ 单击“确定”按钮，返回“安全”选项卡。在“组或用户名”列表框中，选择 HRA 计算机的名称，然后在权限列表框中选中“请求证书”和“颁发和管理证书”复选框。如果使用自动 CA 数据库管理，则需要选中“管理 CA”复选框，如图 14-20 所示。

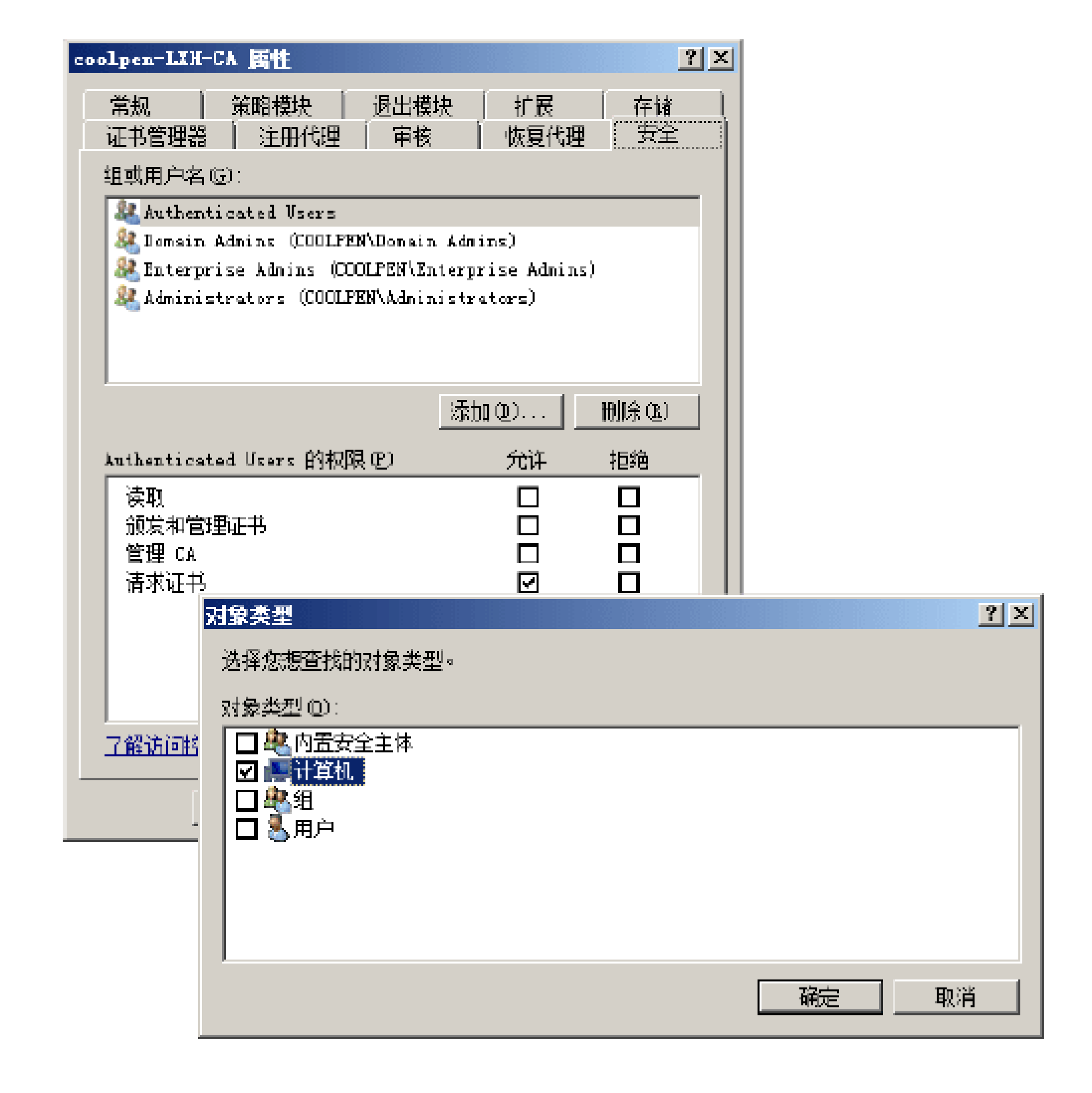


图 14-19 “对象类型”对话框

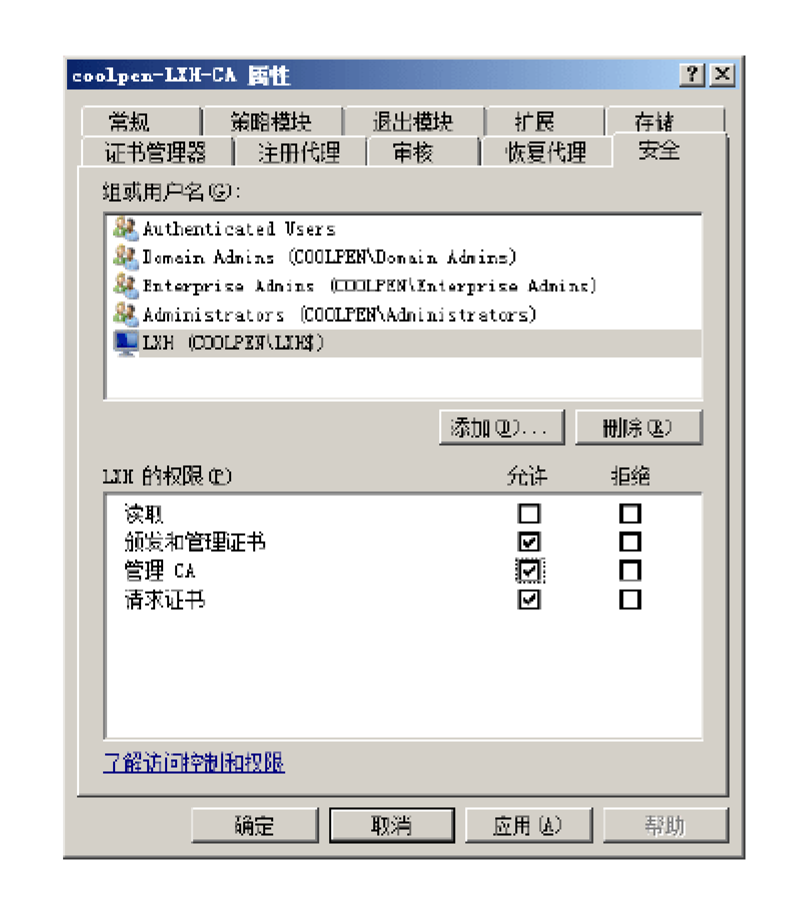


图 14-20 选择权限

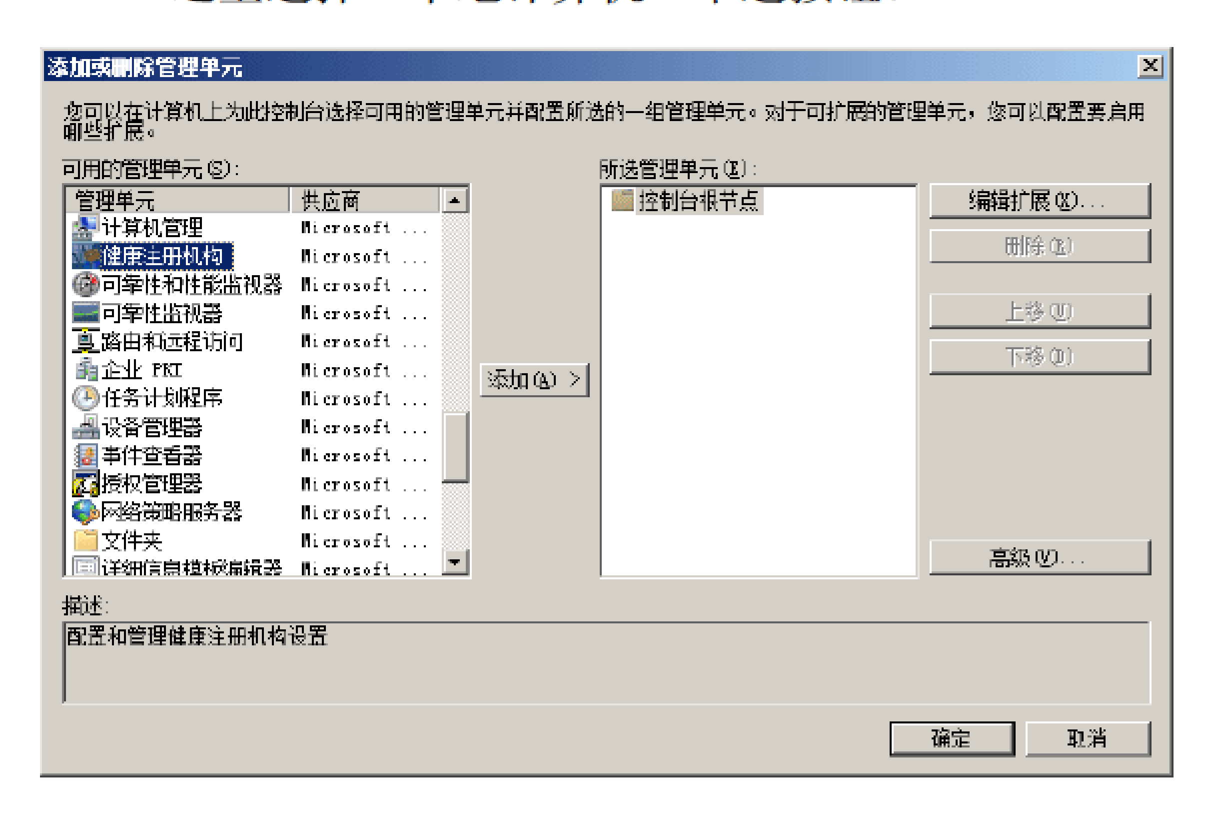
⑤ 单击“确定”按钮，保存设置，并关闭该属性对话框。

3. 配置 HRA 的属性

每个 HRA 计算机必须使用 NAP CA 顺序列表来配置，为 NAP 客户端请求健康证书。

① 选择“开始”→“运行”命令，在“打开”文本框中输入“MMC”，按 Enter 键确认，打开管理控制台窗口。依次选择“文件”→“添加/删除管理单元”命令，显示如图 14-21 所示的“添加或删除管理单元”对话框。在“可用的管理单元”列表框中，选择“健康注册机构”选项。

② 单击“添加”按钮，显示如图 14-22 所示的“健康注册机构”对话框。根据需要选择所要的选项，这里选择“本地计算机”单选按钮。



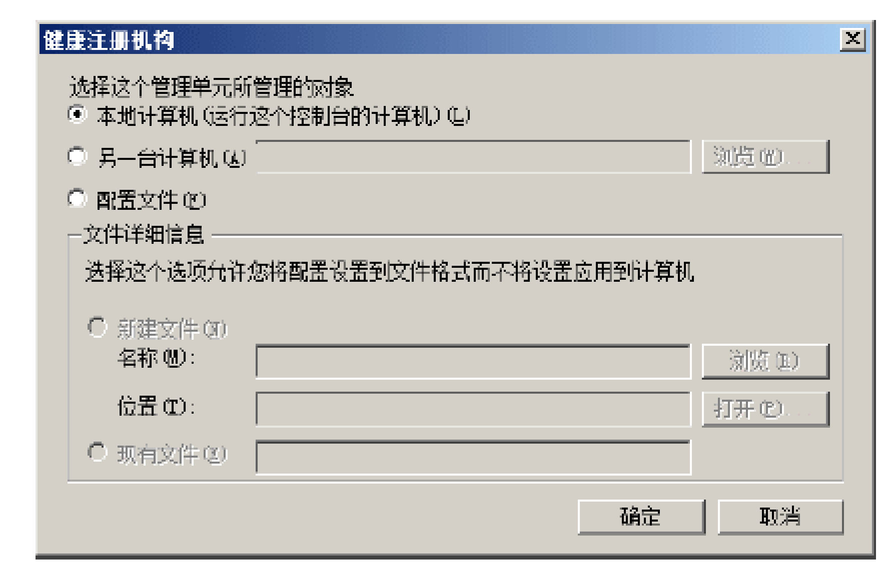
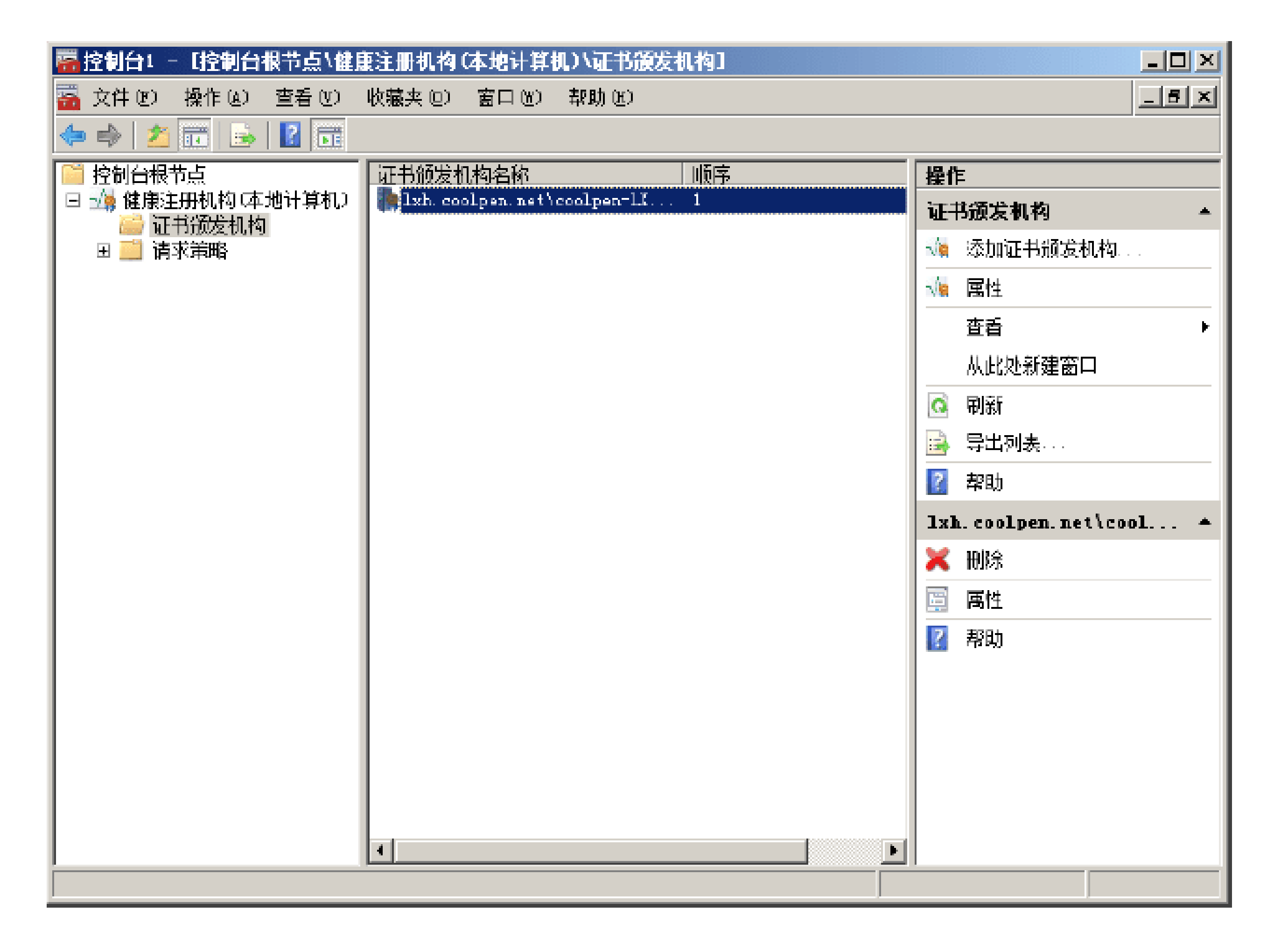


图 14-21　“添加或删除管理单元”对话框　　　　图 14-22　“健康注册机构”对话框

③ 单击“确定”按钮，确认并返回“添加或删除管理单元”对话框。再次单击“确定”按钮，返回管理控制台窗口，如图 14-23 所示。在左侧栏中，展开“健康注册机构”节点，在中间栏中选择所要配置的证书颁发机构。

④ 在右侧栏中，单击“属性”按钮，显示如图 14-24 所示的“证书颁发机构属性”对话框。在“设置”选项卡中，指定适当的设置如 HRA 要求的健康证书的有效时间，以及 HRA 是否使用独立或企业 CA。



证书颁发机构属性
设置
当服务器被标识为不可用时请求之间的分钟数(M)
由此健康注册机构批准的证书将有效(C):
4
小时
使用独立证书颁发机构(S)
启用 PolicyOID(O)
使用企业证书颁发机构(E)
确定
取消
应用(A)

图 14-23　“健康注册机构”管理单元　　　　图 14-24　“证书颁发机构属性”对话框

⑤ 单击“确定”按钮，保存设置。

4. 作为 RADIUS 代理在 HRA 上配置 NPS 服务

如果 NAP 健康策略服务器与 HRA 计算机位于不同的服务器上，则必须在 HRA 计算机上配置 NPS 服务作为 RADIUS 代理。允许 HRA 计算机作为 RADIUS 客户端，将基于 RADIUS 的请求发送到 NAP 健康策略服务器。

14.1.3 配置 NAP 健康策略服务器

为了配置 NAP 健康策略服务器，需要执行如下操作：

- 添加网络策略和访问服务角色。
- 安装 SHV。
- 配置 RADIUS 服务器设置。
- 为 IPSec 强制配置健康要求策略。

1. 配置 RADIUS 服务器设置

每个 NAP 健康策略服务器都是一个 RADIUS 服务，可能需要进行如下 RADIUS 服务器的设置。

- RADIUS 通讯的 UDP 端口：通常只有在 NAP 健康策略服务也作为 RADIUS 服务器使用，并且其他 RADIUS 客户端使用与 RFC 定义的不同的端口时，才需要该步骤。NAP 健康策略服务器所使用的默认端口与 HRA 使用的端口相同。
- RADIUS 日志：用户可以在本地文件或 SQL 数据库服务器中配置 NPS 服务来记录入站请求和记账信息。

需要注意的是，必须使用 HRA 配置每个 NAP 健康策略服务器作为 RADIUS 客户端。

① 在“网络策略服务器”管理单元中，展开“RADIUS 客户端和服务器”节点，右击“RADIUS 客户端”并在弹出的快捷菜单中选择“新建 RADIUS 客户端”命令，显示如图 14-25 所示的“新建 RADIUS 客户端”对话框。

② 在“友好名称”文本框中，输入 HRA 计算机的名称。在“地址(IP 或 DNS)”文本框中，输入 HRA 计算机的 IPv4 地址、IPv6 地址或 DNS 域名称。如果输入 DNS 域名称，需要单击“验证”按钮来解析名称为 IP 地址。

③ 在“共享机密”选项区域的“共享机密”和“确认共享机密”文本框中，输入 NPS 服务器和 HRA 计算机联合的共享机密，或者选择“生成”单选按钮使 NPS 服务生成一个 RADIUS 共享机密。

④ 选中“RADIUS 客户端支持 NAP”复选框。

⑤ 单击“确定”按钮，确认并保存设置。为每个 HRA 重复以上步骤，发送健康评估请求到 NAP 健康策略服务器。

2. 为 IPSec 强制配置健康要求策略

创建健康要求策略，可以通过手动和“配置 NAP 向导”两种方式完成，具体创建操作参见前面相关内容，这里不再赘述。因为 NAP 客户端的默认网络策略模式为只允许受限访问(强制方法)模式，因此，必须为不符合的 NAP 客户端的完全访问修改网络策略。

① 在“网络策略服务器”管理单元中，展开“策略”节点，选择“网络策略”选项。如果在“选择与 NAP 一起使用的网络连接方法”中使用 IPSec 作为名称，那么不符合的 NAP 客户端的网络策略

名称就是 IPSec 不符合，如图 14-26 所示。

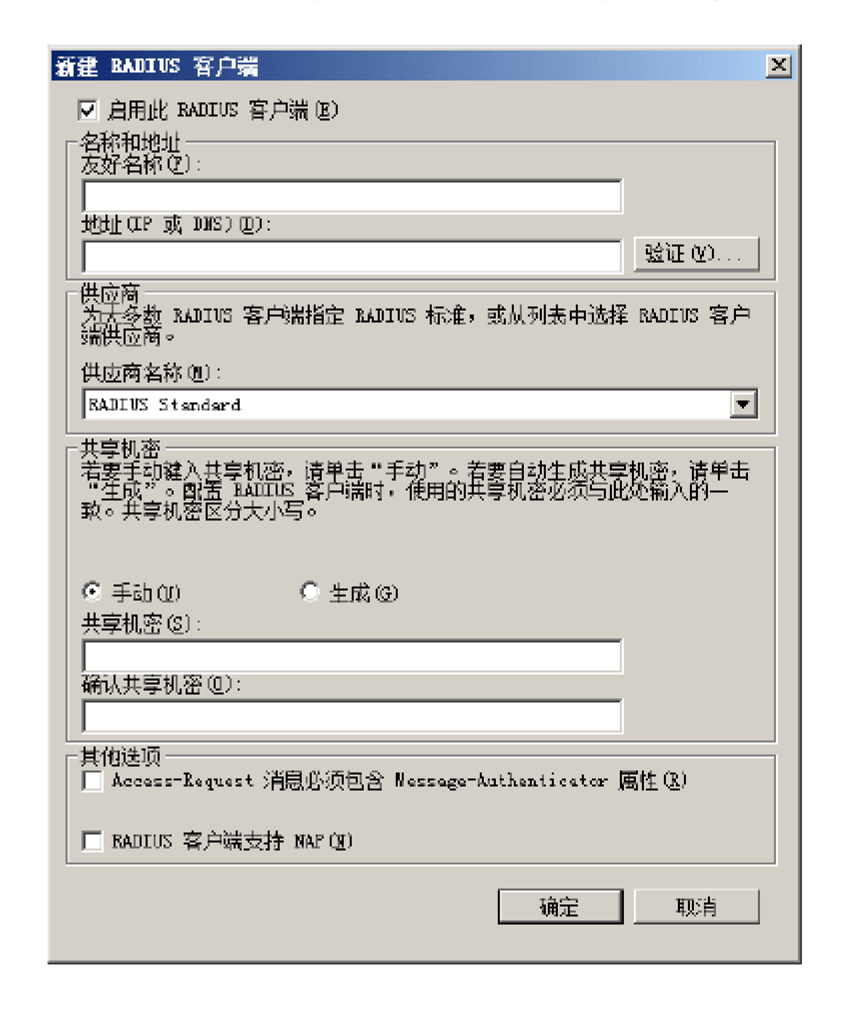


图 14-25　“新建 RADIUS 客户端”对话框

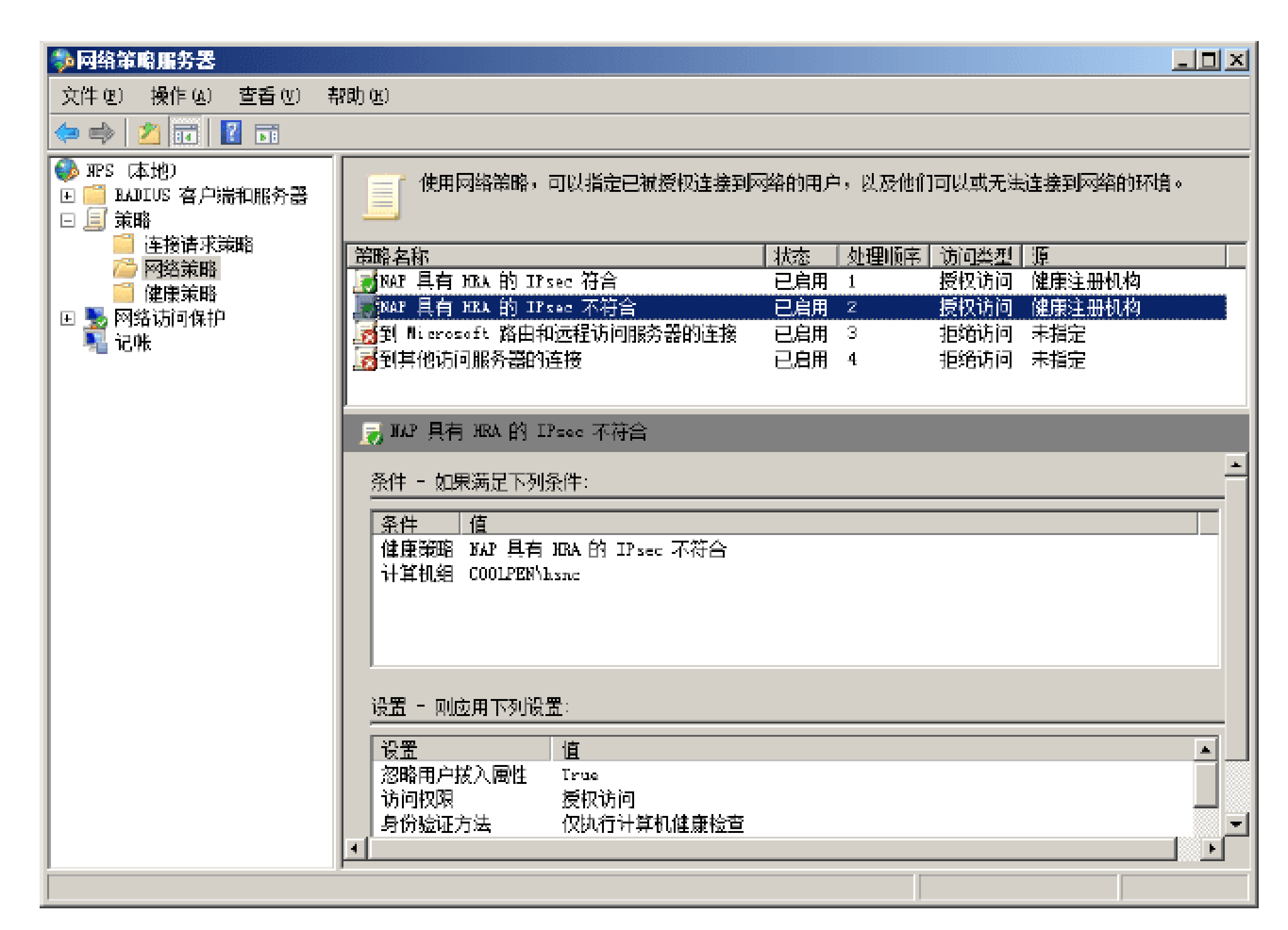


图 14-26　“网络策略服务器”对话框

② 双击 NAP 向导为不符合的 NAP 客户端创建的网络策略，打开“NAP 具有 HRA 的 IPSec 不符合 属性”对话框，切换至“设置”选项卡，选择“NAP 强制”，如图 14-27 所示。在右侧栏中，选择“允许完全网络访问”单选按钮。

③ 单击“确定”按钮，保存设置。

3. 配置 SHV

① 在“网络策略服务器”管理单元中，依次展开“网络访问保护”→“系统健康验证器”节点，在右侧栏中，双击 SHV，然后配置每个 SHV 的系统健康要求。例如，双击“Windows 安全健康验证程序”，显示如图 14-28 所示的“Windows 安全健康验证程序 属性”对话框。

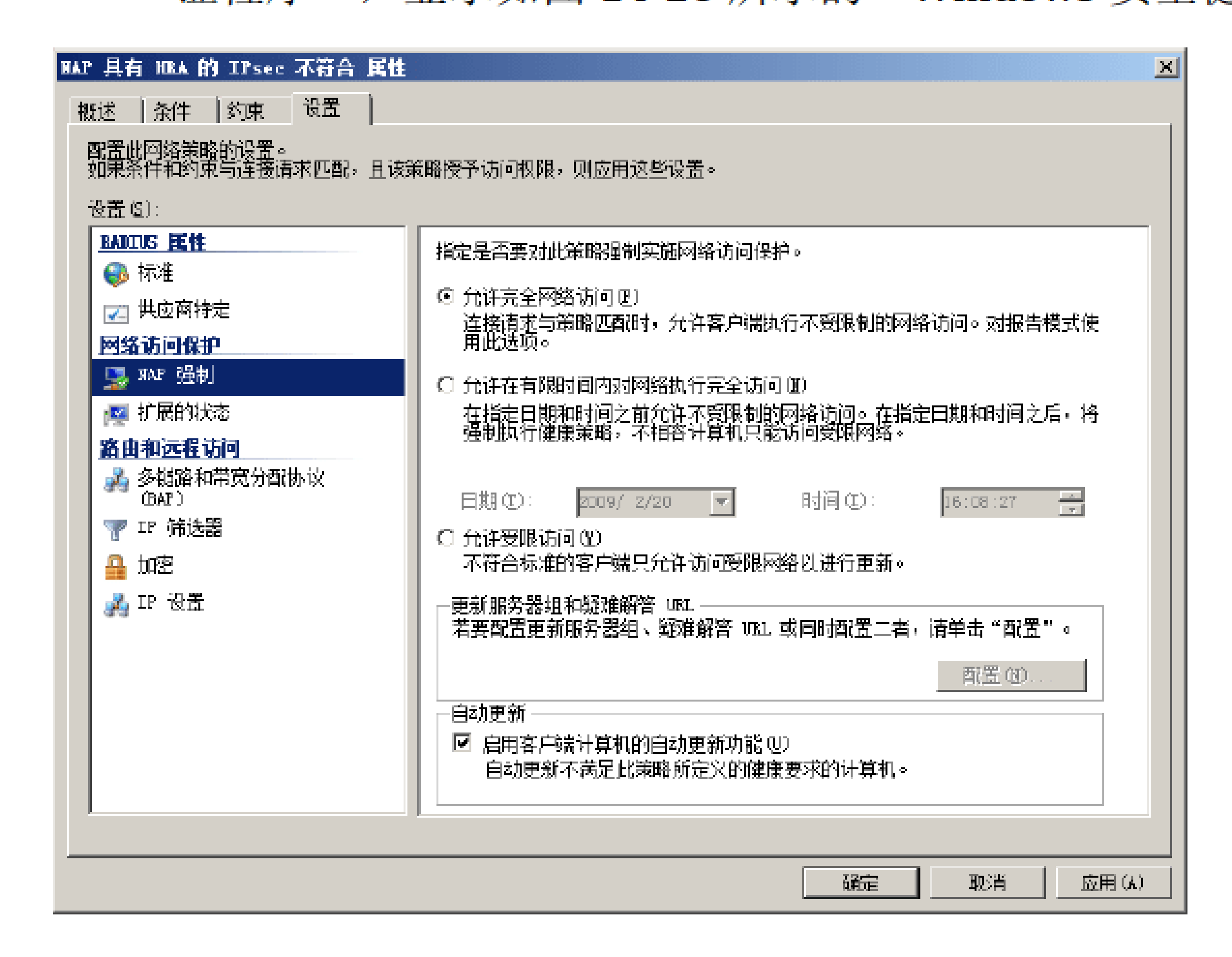


图 14-27　“NAP 具有 HRA 的 IPSec 不符合 属性”对话框

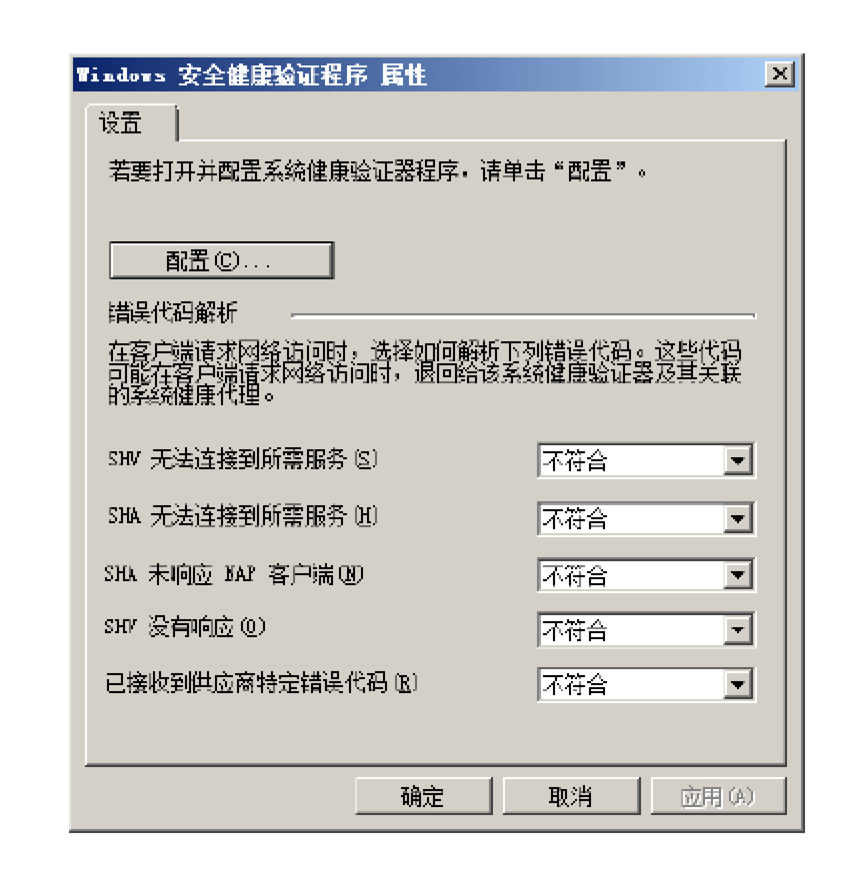


图 14-28　“Windows 安全健康验证程序 属性”对话框

② 单击“配置”按钮，显示如图 14-29 所示的“Windows 安全健康验证程序”对话框，根据需要配置基于 Windows Vista 和 Windows XP 的系统健康要求即可。

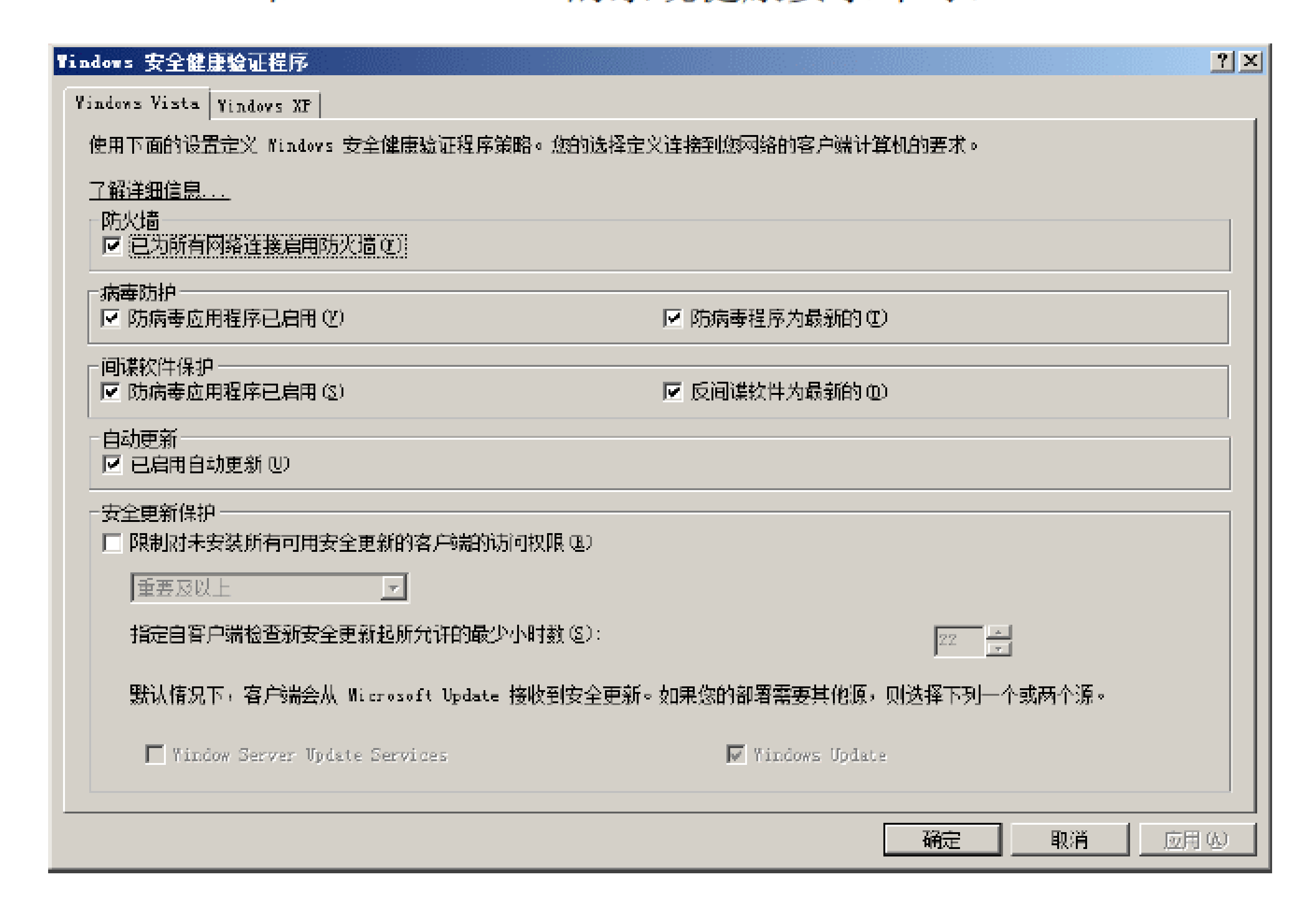


图 14-29 “Windows 安全健康验证程序”对话框



提示：确保健康策略配置了正确的 SHV，以及影响健康要求的条件，还可以对健康策略中的每个条件进行选择。

③ 配置完成后，单击“确定”按钮，保存设置。

14.1.4 配置 NAP 客户端

为了配置 NAP 客户端，需要执行如下任务：

- 通过组策略配置 NAP 客户端。
- 配置 HRA 的 DNS 发现(根据需要)。
- 添加 NAP 客户端到安全网络。

1. 通过组策略配置 NAP 客户端

尽管可以单独配置 NAP 客户端，但是在活动目录域环境中，建议使用集中配置 NAP 客户端的方式。通常情况下是通过组策略设置，主要包括如下任务：

- 配置 NAP 客户端设置。
- 启用 Windows 安全中心。
- 配置网络访问保护代理服务的自动启用。

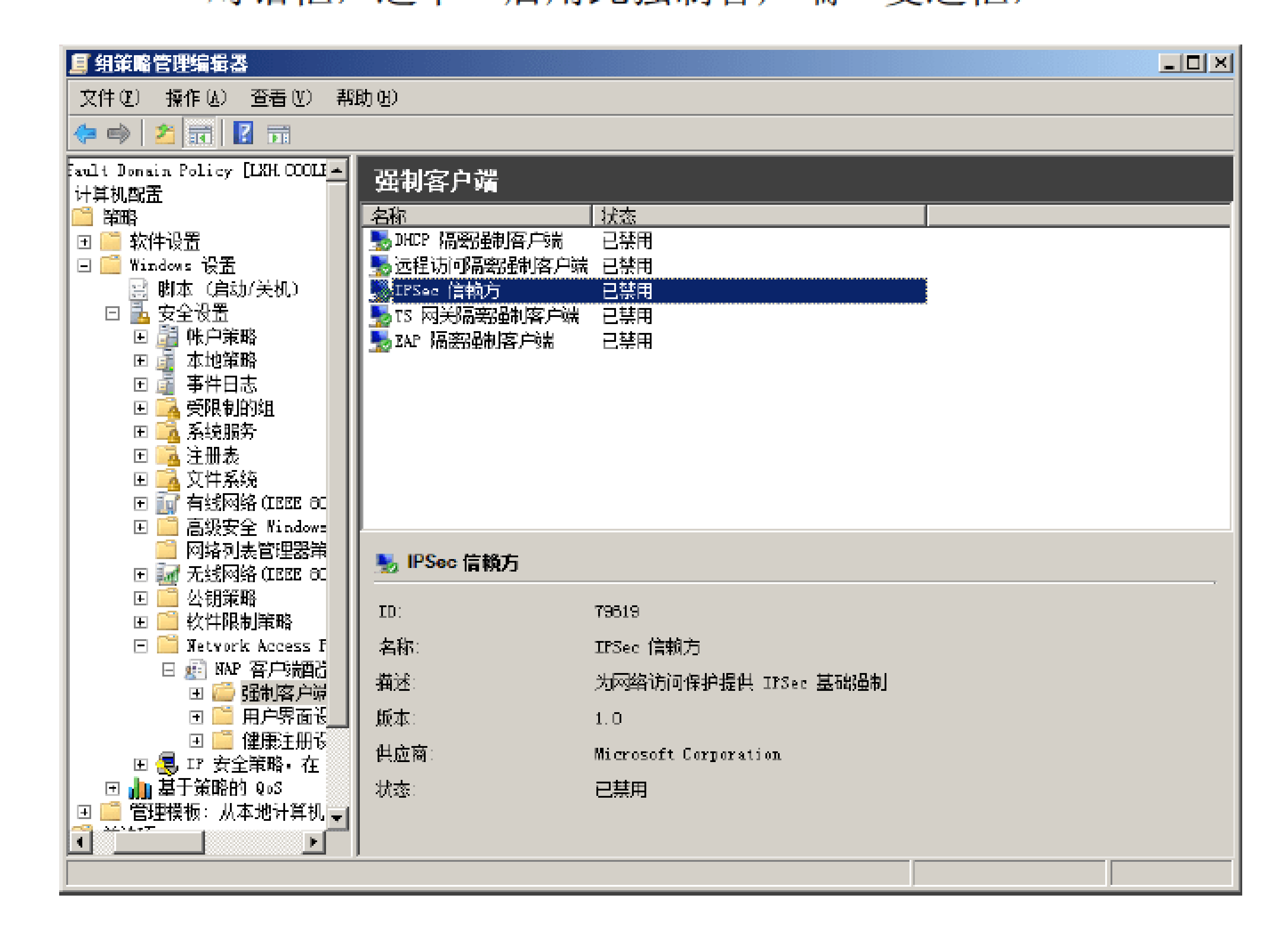
(1) 配置 NAP 客户端的设置

① 在“组策略管理器”管理单元中，依次展开“林”→“域”节点。在“链接的组策略对象”面板中，右击组策略对象(默认对象是 Default Domain Policy)，在弹出的快捷菜单中选择“编辑”选项，打开“组策略管理编辑器”窗口。

② 依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→Network Access Protection

→“NAP 客户端配置”→“强制客户端”节点，如图 14-30 所示。

③　在右侧栏中，双击“IPSec 信赖方”强制客户端，显示如图 14-31 所示的“IPSec 信赖方 属性”对话框，选中“启用此强制客户端”复选框，



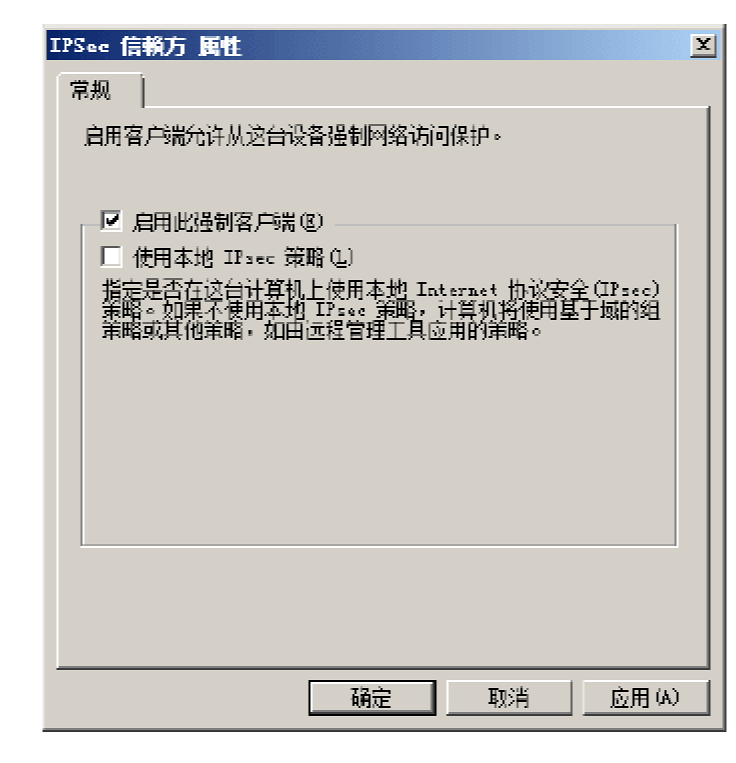


图 14-30　展开“强制客户端”　　　　图 14-31　“IPSec 信赖方 属性”对话框

④　单击“确定”按钮，保存设置。

⑤　如果使用受信任的服务器组作为 NAP 客户端查找 HRA 的方法，则可在控制台中展开“健康注册设置”节点，如图 14-32 所示。



图 14-32　展开“健康注册设置”

⑥　添加受信任服务器组。右击“受信任服务器组”，在弹出的快捷菜单中选择“新建”命令，显示如图 14-33 所示的“组名”对话框。在“组名”文本框中，输入组的名称。

⑦　单击“下一步”按钮，显示如图 14-34 所示的“添加服务器”界面。根据需要在“添加您希望客户端信任的注册机构的 URL(L)”文本框中，输入为应用组策略对象的 NAP 客户端所使用的 HRA

URL。

- 为使用 SSL 的 HTTP 认证健康证书，URL 必须采用如下形式：
  https://HRA_FQDN/domainhra/hcsrvext.dll(其中 HRA_FQDN 为 HRA 计算机的 FQDN)
- 为认证使用 HTTP 的健康证书，URL 必须采用如下形式：
  http://HRA_FQDN/domainhra/hcsrvext.dll
- 为认证使用通过 SSL 的 HTTP 的匿名健康证书，URL 必须采用如下形式：
  https://HRA_FQDN/nondomainhra/hcsrvext.dll
- 为认证使用 HTTP 的匿名健康证书，URL 必须采用如下形式：
  http://HRA_FQDN/nondomainhra/hcsrvext.dll

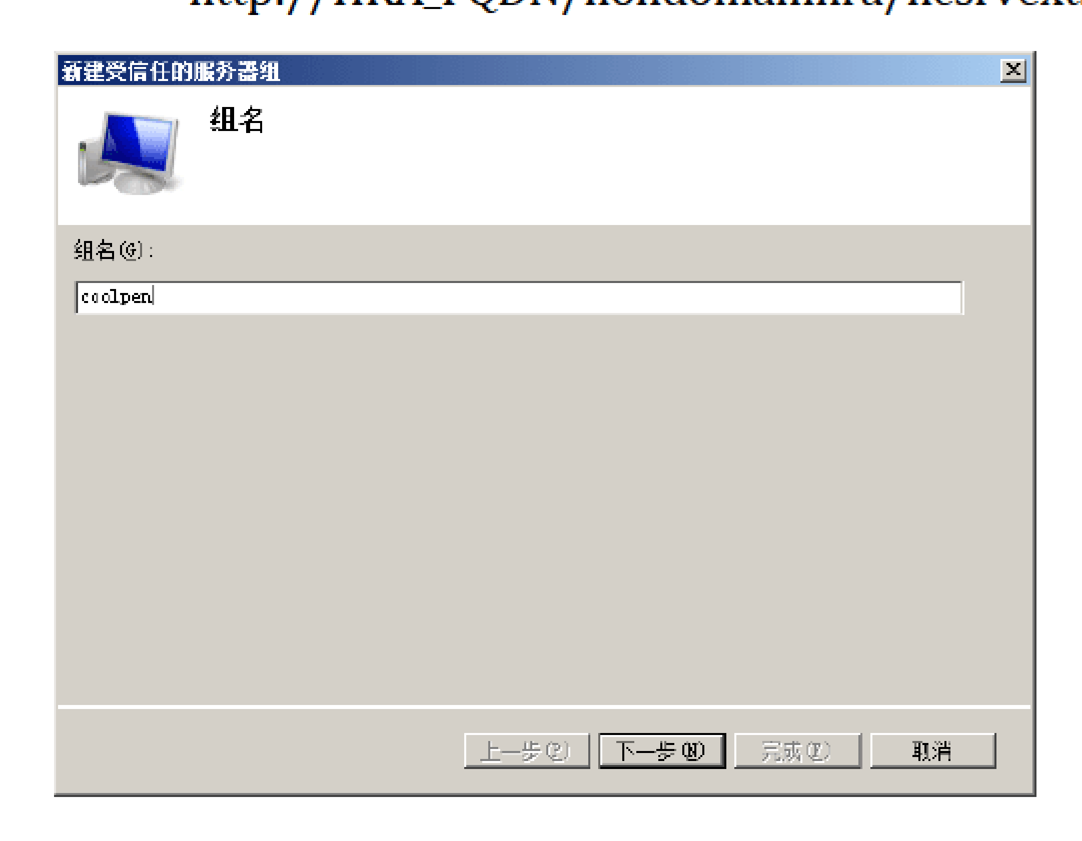


图 14-33 “组名”对话框



图 14-34 “添加服务器”界面

如果想要所有 URL 都基于 SSL，则需要选中“要求对此组中的所有服务器进行服务器验证(https:)”复选框。如果有任意一个 URL 不是基于 SSL 的，则取消选中“要求对此组中的所有服务器进行服务器验证(https:)”复选框即可。如图 14-35 所示为当所有 URL 都是基于 SSL 的实例。

⑧ 验证列表中的所有 URL 是否按照正确的顺序，如不正确，可以单击“上移”、“下移”按钮来更正。

⑨ 单击“下一步”按钮，显示如图 14-36 所示的“正在完成新建受信任的服务器组向导”界面。



图 14-35 配置基于 SSL 的 URL 的实例



图 14-36 “正在完成新建受信任的服务器组向导”界面

⑩　单击“完成”按钮，完成添加受信任服务器组的操作。

(2)　启用 Windows 安全中心

为了使用组策略启用 NAP 客户端上的 Windows 安全中心，可按如下步骤操作。

在“组策略管理编辑器”管理单元中，依次展开“计算机配置”→“策略”→“管理模板”→“Windows 组件”→“安全中心”节点，如图 14-37 所示。双击“启用安全中心(仅限域 PC)”，显示“启用安全中心(仅限域 PC)属性”对话框，选择“已启用”单选按钮。最后，单击“确定”按钮，保存设置即可。

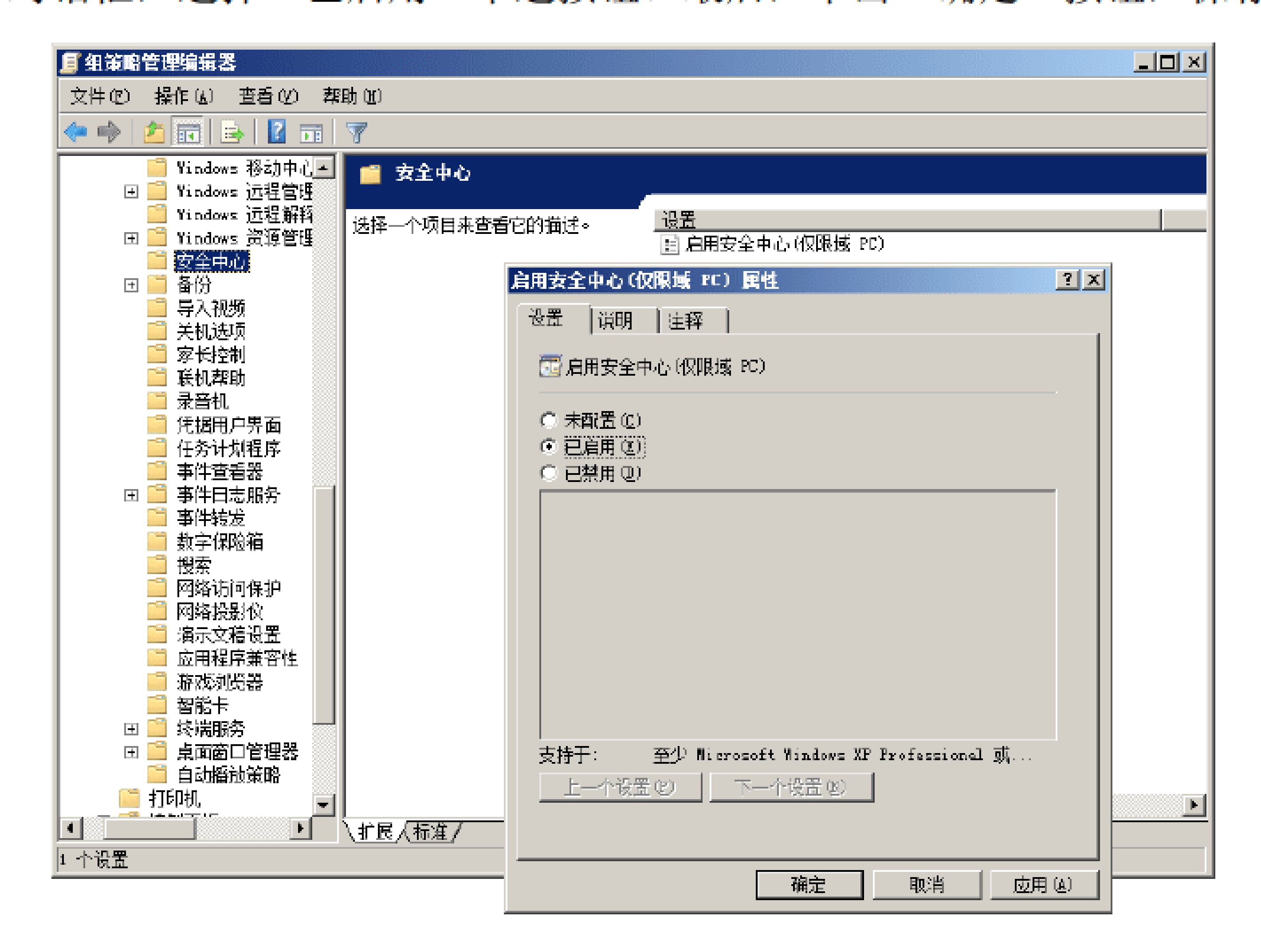


图 14-37　“安全中心”窗口

(3)　配置网络访问保护代理服务的自动启用

在“组策略管理编辑器”管理单元中，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“系统服务”节点。在详细面板中，双击 Network Access Protection Agent 选项，显示如图 14-38 所示的“Network Access Protection Agent 属性”对话框。选中“定义这个策略设置”复选框，并选择“自动”单选按钮。

单击“确定”按钮，保存设置。

2. 配置 HRA 的 DNS 发现

当使用组策略设置 NAP 客户端时，为了使用 DNS SRV 记录来配置 NAP 客户端发现 HRA，需要进行如下操作。

①　从 NAP 客户端组策略设置中删除所有已有受信任服务器组的配置。如果这些设置存在，NAP 客户端将不会使用 DNS SRV 记录来尝试发现 HRA。

②　在 NAP 客户端计算机上，创建和设置 HKLM\SOFTWARE\Policies\Microsoft\NetworkAccessProtection\ClientConfig\Enroll\HcsGroups\EnableDiscovery 的值为 1。

3. 添加 NAP 客户端到安全网络

如果用户没有使用计算机 OU 作为安全网络 OU，则使用“活动目录用户和计算机”管理单元将 NAP 客户端的计算机账户放置在安全网络 OU 或安全组中。

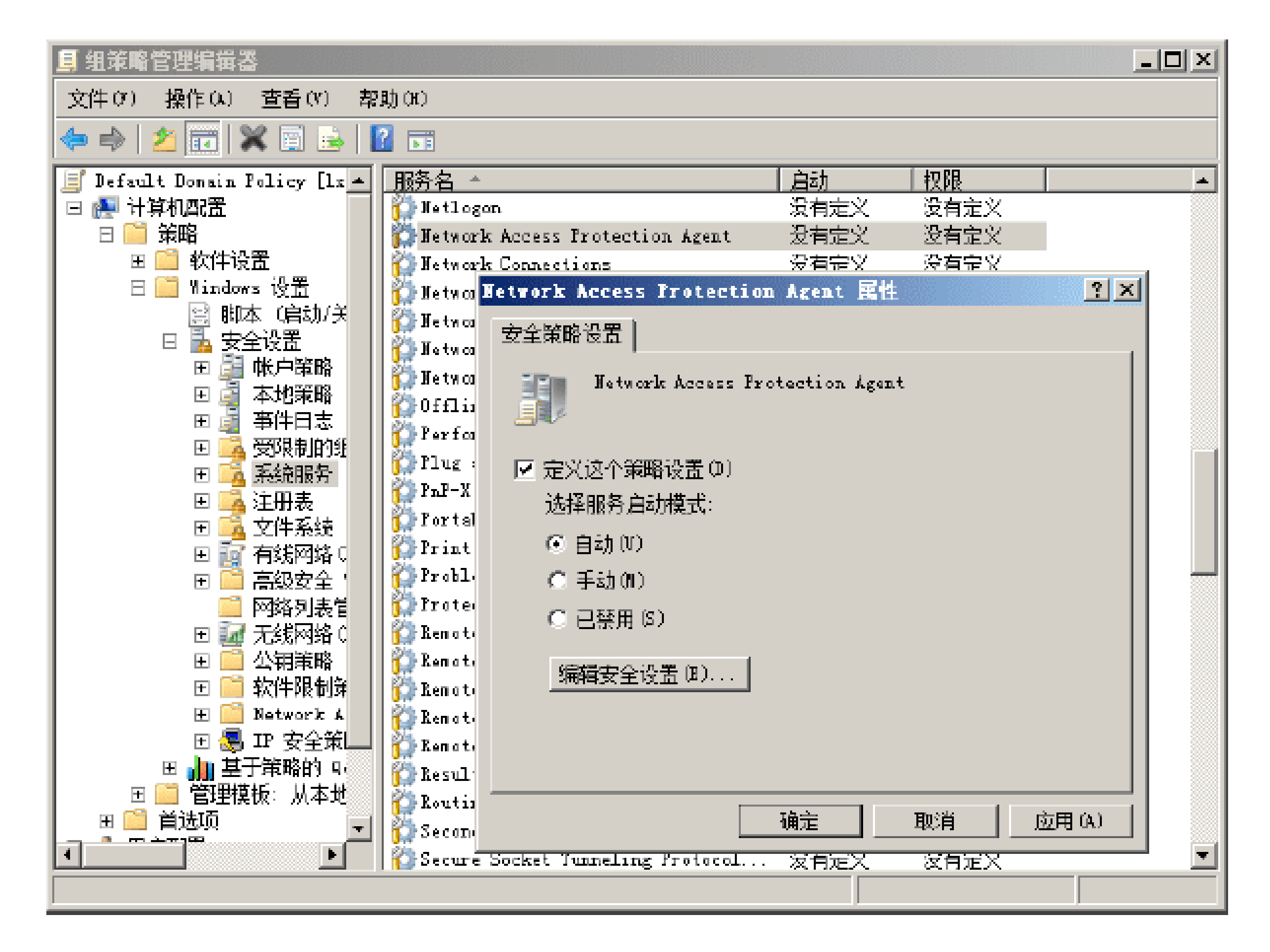


图 14-38 “Network Access Protection Agent 属性”对话框

14.1.5 配置和应用 IPSec 策略

在验证了 NAP 客户端收到短期的健康证书和更新服务器收到长期的健康证书后，即可开始配置和应用 IPSec 策略到边界和安全网络中的计算机上。这需要执行如下操作。

① 为边界网络配置和应用 IPSec 策略设置。

② 测试清空文本和与边界网络计算机的受保护的通信。

③ 为安全网络中的部分计算机配置和应用 IPSec 策略设置。

④ 测试清空文本和与安全网络计算机的受保护的通信。

⑤ 为延期强制模式下的不符合的 NAP 客户端配置网络策略。

⑥ 为安全网络中所有的计算机配置和应用 IPSec 策略。

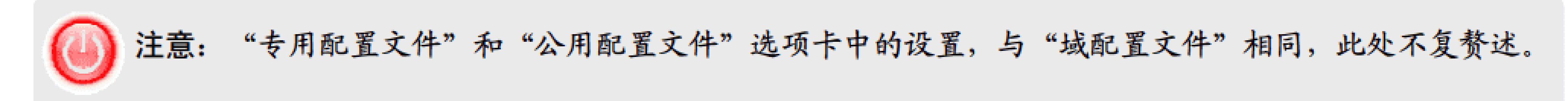
⑦ 为强制模式下的不符合的 NAP 客户端配置网络策略。

1. 为边界网络配置和应用 IPSec 策略设置

在这里需要创建包含 IPSec 策略设置的 GPO，请求为边界网络计算机的入站和出站通信进行 IPSec 保护。

① 在 Windows Server 2008 域控制器上，打开指定 GPO 的“组策略管理编辑器”窗口，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“高级安全 Windows 防火墙”→“高级安全 Windows 防火墙-LDAP”节点，如图 14-39 所示。

② 右击“高级安全 Windows 防火墙-LDAP”，在弹出的快捷菜单中选择“属性”命令，显示如图 14-40 所示的“高级安全 Windows 防火墙-LDAP”属性对话框。在“域配置文件”选项卡的“防火墙状态”下拉列表中选择“启用(推荐)”选项，在“入站连接”下拉列表框中选择“阻止(默认值)”选项，在“出站连接”下拉列表中选择“允许(默认值)”选项。



注意：“专用配置文件”和“公用配置文件”选项卡中的设置，与“域配置文件”相同，此处不复赘述。

③ 单击“确定”按钮，保存配置。



图 14-39　展开“高级安全 Windows 防火墙-LDAP”



图 14-40　“高级安全 Windows 防火墙-LDAP”属性对话框

④ 在“高级安全 Windows 防火墙-LDAP”节点中，右击“连接安全规则”并在弹出的快捷菜单中选择“新规则”命令，显示“规则类型”对话框，选择“隔离”单选按钮。单击“下一步”按钮，显示如图 14-41 所示的“要求”界面，选择“入站和出站连接请求身份验证”单选按钮。



图 14-41　“要求”界面

⑤ 单击“下一步”按钮，显示如图 14-42 所示的“身份验证方法”界面。选择“计算机证书”单选按钮，然后单击“浏览”按钮，查看并选择所使用的证书，并选中“只接受健康证书”复选框。

⑥ 单击“下一步”按钮，显示如图 14-43 所示的“配置文件”界面。选中“域”、“专用”和“公用”复选框。



图 14-42 “身份验证方法”界面



图 14-43 “配置文件”界面

⑦ 单击“下一步”按钮，显示如图 14-44 所示的“名称”界面。在“名称”文本框中，输入该规则的名称。在“描述”文本框中，输入该规则的描述信息。

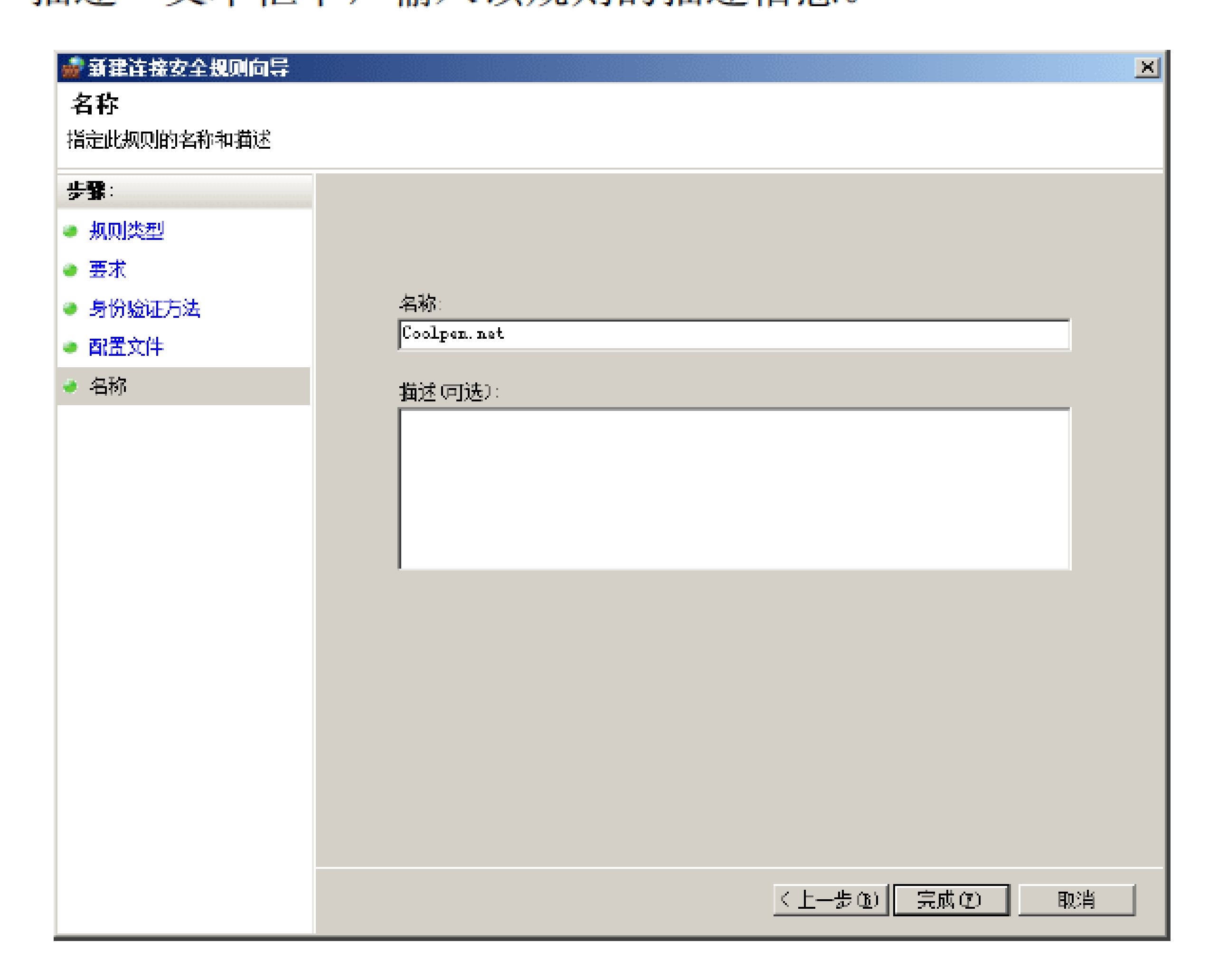


图 14-44 “名称”界面

⑧ 单击“完成”按钮，完成新规则的配置。在创建完边界网络 GPO 后，需要将其应用于边界网络 OU 或安全组。

2. 测试与边界网络计算机的通信

在应用边界网络 GPO 到边界网络安全组或 OU 后，需要完成如下工作：

- 确保边界网络中的更新服务器能够收到边界网络 GPO 设置，并且拥有为入站和出站通讯请求 IPSec 保护的连接安全规则。
- 如果更新服务器可以收到边界网络 GPO 的设置，确保更新服务器可以建立与 NAP 客户端和非域

成员计算机的通信，并且 NAP 客户端和非域成员计算机可以建立与更新服务器的通信。

在该阶段的 NAP 客户端、非域成员计算机和更新服务器之间的通信应该清除文本。更新服务器上的 IPSec 策略将会尝试越过 IPSec 保护，但是允许回退清除入站和出站通信尝试。

3. 为安全网络中部分计算机配置和应用 IPSec 策略设置

在应用安全网络 GPO 到所有域成员计算机之前，用户应该在部分域成员计算机上测试安全网络 GPO，并且记录通信动作。可以使用如下方式实现：

- 包含测试计算机的安全测试网络 OU。在这种情况下，用户可以直接应用安全网络 GPO 到安全测试网络 OU 上，而不会影响到其他计算机。
- 包含测试计算机的安全测试网络安全组。在这种情况下，用户必须为安全测试网络安全组筛选 GPO 的作用域，应用安全网络 GPO 到安全网络 OU 上。因为作用域的筛选，安全网络 GPO 将只会应用于安全测试网络安全组的成员上。

这里创建包括 IPSec 策略设置的 GPO，为安全网络计算机的入站和出站通信尝试提供 IPSec 保护。

① 在安装了组策略管理器的 Windows Server 2008 计算机上，打开 MMC 管理控制台，依次选择“开始”→“添加/删除管理单元”命令，显示“添加或删除管理单元”对话框。在“可用的管理单元”列表框中，选择“组策略管理编辑器”选项。

② 单击“添加”按钮，显示“浏览组策略对象”对话框。单击“浏览”按钮，查看并选择所要编辑的组策略，如图 14-45 所示。单击“创建新的组策略对象”按钮，输入安全网络的新的组策略对象的名称。

③ 单击“确定”按钮，返回“选择组策略对象”对话框。单击“完成”按钮，返回“添加或删除管理单元”对话框。再次单击“确定”按钮，完成管理单元的添加。

④ 在控制台中，展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“高级安全 Windows 防火墙”→“高级安全 Windows 防火墙-LDAP”节点。右击“高级安全 Windows 防火墙-LDAP”，在弹出的快捷菜单中选择“属性”命令。打开“高级安全 Windows 防火墙-LDAP”对话框。在“域配置文件”选项卡中，在“防火墙状态”下拉列表框中选择“启用(推荐)”选项，在“入站连接”下拉列表框中选择“阻止(默认值)”选项，在“出站连接”下拉列表框中选择“允许(默认值)”选项。



图 14-45　“浏览组策略对象”对话框

⑤ 切换到“专有配置文件”选项卡，在“防火墙状态”下拉列表框中选择“启用(推荐)”选项，在“入站连接”下拉列表框中选择“阻止(默认值)”选项，在“出站连接”下拉列表框中选择“允许(默认值)”选项。

⑥ 切换到“公用配置文件”选项卡，在“防火墙状态”下拉列表框中选择“启用(推荐)”选项，在“入站连接”下拉列表框中选择“阻止(默认值)”选项，在“出站连接”下拉列表框中选择“允许(默认值)”选项。

⑦ 单击“确定”按钮，保存设置。

⑧ 在“高级安全 Windows 防火墙-LDAP”中，右击“连接安全规则”，在弹出的快捷菜单中选择“新规则”命令，打开“规则类型”对话框，选择“隔离”单选按钮。

⑨ 单击“下一步”按钮，显示如图 14-46 所示的“要求”界面，选择“入站连接要求身份验证，出站连接请求身份验证”单选按钮。



图 14-46 “要求”界面

⑩ 单击“下一步”按钮，打开“身份验证方法”对话框。选择“计算机证书”单选按钮，并选中“只接受健康证书”复选框，然后单击“浏览”按钮，查看并选择证书。

⑪ 单击“下一步”按钮，打开“配置文件”对话框，同时选中“域”、“专用”和“公用”复选框。

⑫ 单击“下一步”按钮，显示“名称”对话框。在“名称”文本框中，输入该规则的名称。在“描述”文本框中，输入该规则的描述信息。

对于运行 Windows XP SP3 的 NAP 客户端，必须使用“组策略编辑器”管理单元和活动目录中的“IP 安全策略”中的“计算机配置\策略\Windows 设置\安全设置”来配置和启用同等的 IPSec 策略。另外，还必须设置 HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley\IKEFlags 的注册表值为 0x1c。

4. 测试清除文本与安全网络部分计算机的受保护的通信

在配置完安全网络 GPO，并将其应用到安全测试网络 OU 或安全组后，还必须测试如下类型的通信：

- 确保安全网络中的计算机能够收到安全网络 GPO 设置，并且拥有入站要求 IPSec 保护和出站请求 IPSec 保护的连接安全规则。例如，可以使用安全网络计算机上的“高级安全 Windows 防火墙”管理单元中的“监视器”节点。
- 如果安全网络的计算机可以收到安全网络 GPO 的设置，需确保如下通信动作。
  - 阻止从非安全测试网络的计算机到安全测试网络计算机的通信。
  - 保护从安全测试网络中的计算机到另一个安全测试网络计算机的通信。
  - 允许从安全测试网络计算机到非安全测试网络计算机的通信，但是不被保护。

该阶段的安全测试网络计算机到所有非安全测试网络的计算机通信应该被清除文本。安全测试网络计算机的 IPSec 策略将会尝试越过 IPSec 保护，但是会允许回退清除入站和出站通信尝试。

5. 为延期强制下的不符合的 NAP 客户端配置网络策略

在测试完边界和安全测试网络的通信后，可以为延期强制模式确定日期。在该时间段内，不符合的 NAP

客户端不会收到健康证书，不能建立与符合的 NAP 客户端的通信。在延期强制模式下，不符合的 NAP 客户端仍会收到健康证书，但是用户会收到一条信息，指示计算机不能按照系统健康要求进行动作。

① 在“网络策略服务器”管理单元中，依次展开“策略”→“网络策略”节点。

② 在右侧栏中，双击 NAP 向导创建的不符合的 NAP 客户端的网络策略，打开策略属性对话框。切换到“设置”选项卡，然后选择“NAP 强制”，如图 14-47 所示。在右侧栏中，选择“允许在有限时间内对网络执行完全访问”单选按钮，指定 NAP 健康策略服务器上配置的强制模式的日期和时间。

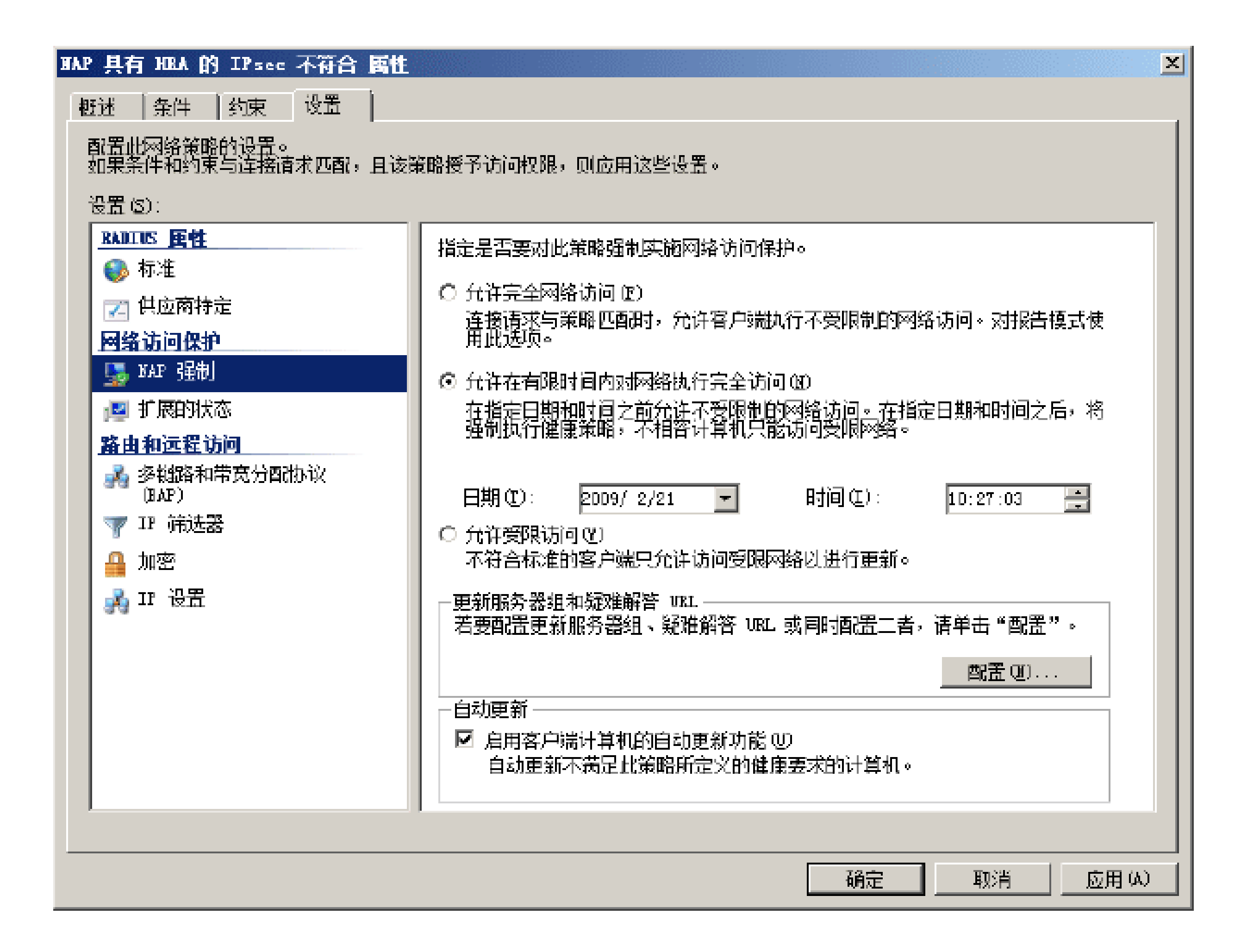


图 14-47　“设置”选项卡

③ 单击“确定”按钮，保存设置。对网络中每个 NAP 健康策略服务器，都需要执行这些操作。

6. 为安全网络中所有计算机配置 IPSec 策略设置

在测试和验证完安全测试网络中的入站和出站通信后，即可应用安全网络 GPO 到安全网络所有计算机上。为了应用安全网络 GPO 到包含所有域成员 NAP 客户端的安全网络 OU 或组，并且保证安全测试网络 OU 或组中的计算机得到适当的移植，具体可通过如下方法实现：

- 如果使用安全测试网络 OU 和包括所有域成员 NAP 客户端的安全网络 OU，则需要应用安全网络 GPO 到安全网络 OU，并且将安全测试网络 OU 中的计算机移植到安全网络 OU 中。
- 如果使用安全测试网络 OU 和包含所有域成员 NAP 客户端的安全网络安全组，则需应用安全网络 GPO 到安全网络 OU 中，并且确保安全测试网络 OU 中的计算机是安全网络 OU 中的成员。
- 如果使用安全测试网络安全组和包含所有域成员 NAP 客户端的安全网络 OU，则需应用安全网络 GPO 到安全网络 OU 中，并且确保安全测试网络安全组中的计算机是安全网络 OU 的成员。
- 如果使用安全测试网络安全组和包含所有域成员 NAP 客户端的安全网络安全组，则应更改安全网络 GPO 的作用域筛选，保证其应用于安全网络安全组中，并且确保安全测试网络安全组中的计算机是安全网络安全组的成员。

7. 为强制模式下的不符合的 NAP 客户端配置网络策略

在强制模式的日期中，配置 NAP 健康策略服务器的强制模式的具体操作步骤如下。

① 在“网络策略服务器”管理单元中，依次展开“策略”→“网络策略”节点。

② 在右侧栏中，双击不符合的 NAP 客户端的网络策略，打开策略属性对话框。切换到“设置”选项卡，然后选择“NAP 强制”，并选择“允许在有限时间内对网络执行完全访问”单选按钮。

③ 单击“确定”按钮，保存设置。

至此，IPSec 强制的配置已经完成，不符合的 NAP 客户端将不会收到健康证书，并且安全网络中的计算机对入站连接请求要求 IPSec 保护和健康证书。

14.2 配置 802.1X 强制

配置 802.1X 强制包括配置活动目录、配置基于 PEAP 的身份验证方式、配置 802.1X 访问点、配置受限网络的更新服务器、配置 NAP 健康策略服务器和配置 NAP 客户端等内容。

14.2.1 配置基于 PEAP 的身份验证方式

如果没有为 802.1X 身份验证的无线或有线访问使用基于 PEAP 的身份验证方式，那么用户必须重新配置访问客户端和 NPS 服务器上的访问策略。在 Windows Server 2008 和 Windows Vista 中，支持如下有线身份验证的 EAP 身份验证方法：

- EAP-TLS
- PEAP-MS-CHAP v2
- PEAP-TLS

EAP-TLS 和 PEAP-TLS 可以与 PKI 和计算机证书、用户证书和智能卡联合使用。使用 EAP-TLS，有线客户端为身份验证发送自己的计算机证书、用户证书或智能卡。

1. 身份验证方法的需求

有线身份验证方法的需求如下：

- EAP-TLS 需要在每台 RADIUS 服务器上安装计算机证书，在所有有线客户端上安装计算机证书、用户证书或智能卡。为了验证 RADIUS 服务器上的计算机证书，RADIUS 服务器计算机证书发布 CA 的根 CA 证书必须安装在所有有线客户端计算机上。为了验证有线客户端的计算机证书、用户证书或智能卡，有线客户端证书的发布 CA 的根 CA 证书必须安装在每台 RADIUS 服务器上。
- PEAP-MS-CHAP v2 需要在每台 RADIUS 服务器上安装计算机证书，并且为了验证 RADIUS 服务器上的计算机证书，RADIUS 服务器计算机证书发布 CA 的根 CA 证书必须安装在所有有线客户端计算机上。

在没有计算机证书、用户证书或智能卡的情况下，可以使用 PEAP-MS-CHAP v2。PEAP-MS-CHAP v2 是一种基于密码的身份验证方法，使用加密的 TLS 会话交换身份验证消息。加密 TLS 会话的使用使得恶意用户很难从捕获的身份验证消息中获取密码。因为 EAP-TLS 和 PEAP-TLS 不依赖于密码，所以它们比 PEAP-MS-CHAP v2 要安全得多。

2. 有线网络(IEEE 802.3)策略组策略扩展

为了使 Windows 有线客户端计算机自动配置有线网络设置，Windows Server 2008 或 Windows Server

2003 活动目录域支持有线网络(IEEE 802.3)策略组策略扩展。该扩展允许将有线网络设置，作为基于域的组策略对象的计算机配置组策略的一部分进行配置。通过使用有线网络(IEEE 802.3)策略组策略扩展，可以在 Windows Server 2008 或 Windows Vista 有线客户端上，指定 EAP 身份验证方法和其他设置。

① 打开相应策略的“组策略对象编辑器”窗口，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“有线网络(IEEE 802.3)策略”节点。默认情况下，没有任何有线网络(IEEE 802.3)策略，根据需要可以创建一个新的策略。右击“有线网络(IEEE 802.3)策略”，在弹出的快捷菜单中选择“创建一个新的 Windows Vista 策略”命令，显示如图 14-48 所示的“新 Vista 有线网络策略 Properties”对话框。

② 在“常规”选项卡中，配置策略的名称和描述，指定是否启用有线自动配置服务。切换到如图 14-49 所示的“安全”选项卡，选中“为网络访问启用 IEEE 802.1X 身份验证”复选框，启用 802.1X 身份验证。根据需要，在“选择网络身份验证方法”下拉列表中，选择所需的身份验证方法。

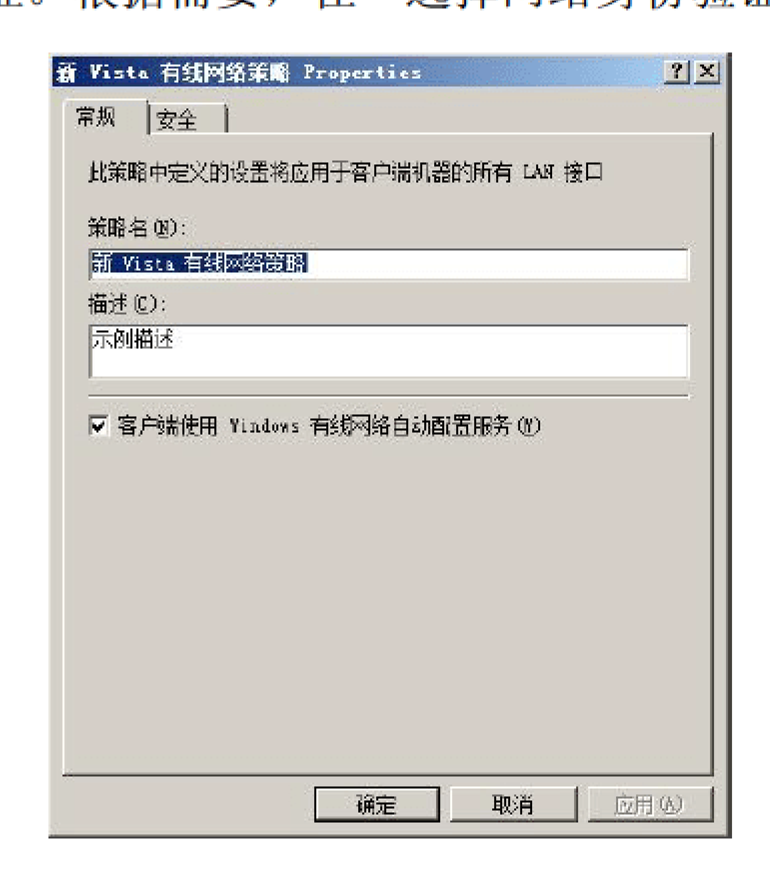


图 14-48 “新 Vista 有线网络策略 Properties”对话框

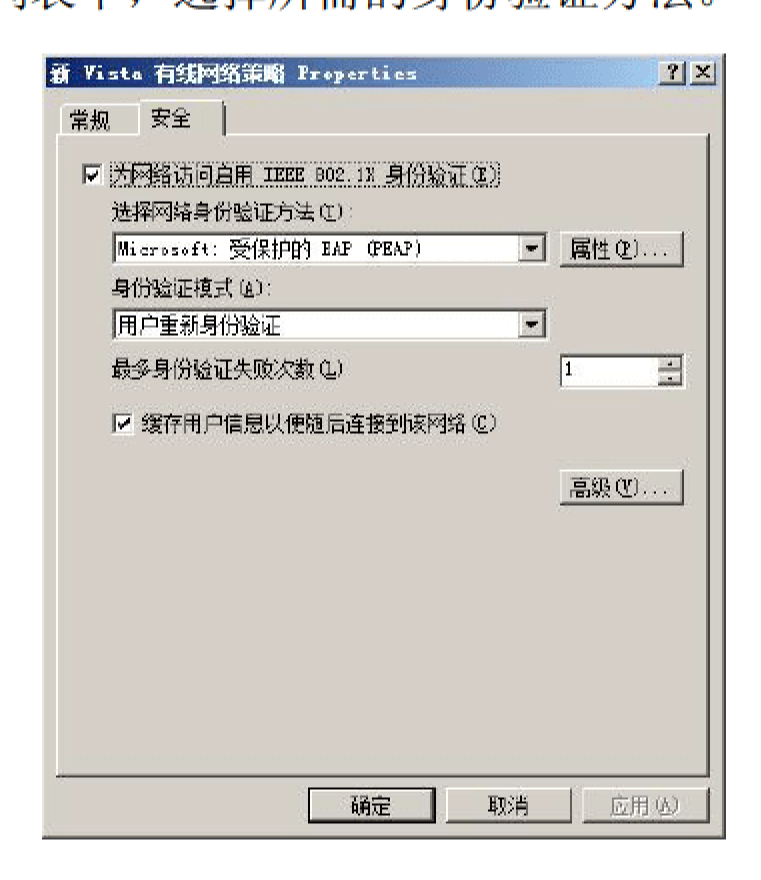


图 14-49 “安全”选项卡

③ 单击“高级”按钮，显示如图 14-50 所示的“高级安全设置”对话框。根据需要，可以配置 802.1X 和单一登录的高级设置。具体各选项含义如下。

■ 最大 Eapol 启动消息数：当发出的最初 EAPOL-Start 消息没有回应时，连续发送的 EAPOL-Start 消息的数目。

■ 保持时间：当最初 EAPOL-Start 消息没有回应时，重发的 EAPOL-Start 消息之间的间隔时间。

■ 启动时间：这段时间内认证客户端将不执行任何 802.1X 身份验证活动。

■ 验证时间：认证客户端在重发 802.1X 请求之前等待的时间。

④ 配置完成后，连续单击“确定”按钮，保存设置。



图 14-50 “高级安全设置”对话框

14.2.2 配置 802.1X 访问点

为了在 802.1X 强制中使用 ACL，需要完成如下工作：

- 使用 ACL 配置 802.1X 访问点，限制不符合的 NAP 客户端的访问。ACL 必须包含符合内网更新服务器通讯的数据包筛选列表。
- 确定通过 802.1X 访问点的 RADIUS 属性识别受限网络访问的 ACL，某些 802.1X 访问使用标准的 RADIUS 属性筛选 ID。
- 为了在 802.1X 强制中使用 VLAN，需要完成如下工作。
  - 如果使用 VLAN 访问内网，那么 VLAN 就变为符合的 NAP 客户端的 VLAN。在这种情况下，只需要为不符合的 NAP 客户端创建一个新的 VLAN 即可。
  - 确定通过 802.1X 访问点的 RADIUS 属性指出受限网络 VLAN，某些 802.1X 访问点使用如下 RADIUS 或指定供应商属性：Tunnel-Medium-Type、Tunnel-Pvt-Group-ID、Tunnel-Type 和 Tunnel-Tag。

14.2.3 配置 NAP 健康策略服务器

802.1X 强制的 NAP 健康策略服务器，与 802.1X 身份验证所使用的基于 NPS 的 RADIUS 服务器相同。关于配置 NAP 健康策略服务器，必须按照如下步骤修改现有 NPS 服务器的配置：

① 安装 SHV。

② 配置 RADIUS 服务器设置。

③ 为 802.1X 强制配置健康要求策略。

1. 配置 RADIUS 服务器设置

由于 NAP 健康策略服务器已经配置了 802.1X 身份验证，所以不需要对 RADIUS 服务器的通常配置进行更改，如 RADIUS 客户端或 UDP 端口。但因为 802.1X 强制配置开始时会使用报告模式，不符合的 NAP 客户端拥有不受限访问，所以要在启用强制模式前使 NAP 健康策略服务器记录入站请求以便于分析。

2. 为 802.1X 强制配置健康要求策略

因为已经拥有 802.1X 身份验证的无线或有线访问的网络策略，为了配置 802.1X 强制的健康要求策略，可以通过如下方式完成：

- 保持已有的无线或有线网络策略，修改该策略使其符合 NAP 客户端，并且为符合的和不符合的 NAP 客户端手动创建新的连接请求策略、健康策略，以及为不符合的和未启用 NAP 的客户端创建其他的网络策略。
- 使用“配置 NAP 向导”为 802.1X 身份验证的无线或有线访问创建新的连接请求策略、网络策略和健康策略，然后手动移植现有的无线和有线网络策略的设置到相应的配置 NAP 向导创建的网络策略中，并再对现有的无线和有线网络策略进行修改。

(1) 为无线或有线连接的 802.1X 强制创建策略

为无线或有线连接的 802.1X 强制创建的策略的操作，可参见第 13 章，其操作基本相同。这里只介绍不同的操作内容。

① 在如图 14-51 所示的“选择与 NAP 一起使用的网络连接方法”界面中，在“网络连接方法”下拉列表框中，选择“IEEE 802.1X(无线)”或者“IEEE 802.1X(有线)”选项，然后在“策略名称”文本框中，输入策略名称。

② 在如图 14-52 所示的“配置身份验证方法”界面中，为 PEAP 身份验证选择 NPS 所使用的计算机

证书，然后根据需要选中“安全密码(PEAP-MS-CHAP v2)”或者“智能卡或其他证书(EAP-TLS)”复选框即可 。

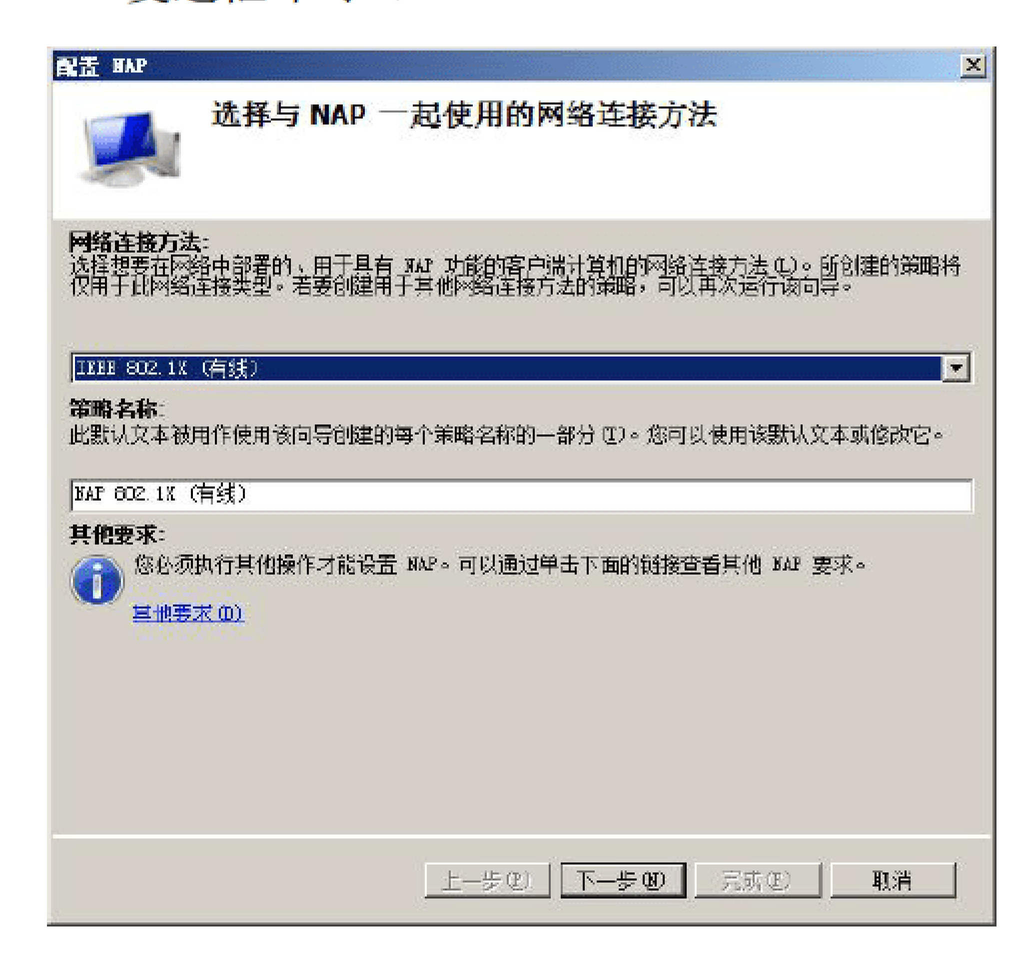


图 14-51　“选择与 NAP 一起使用的网络连接方法”界面

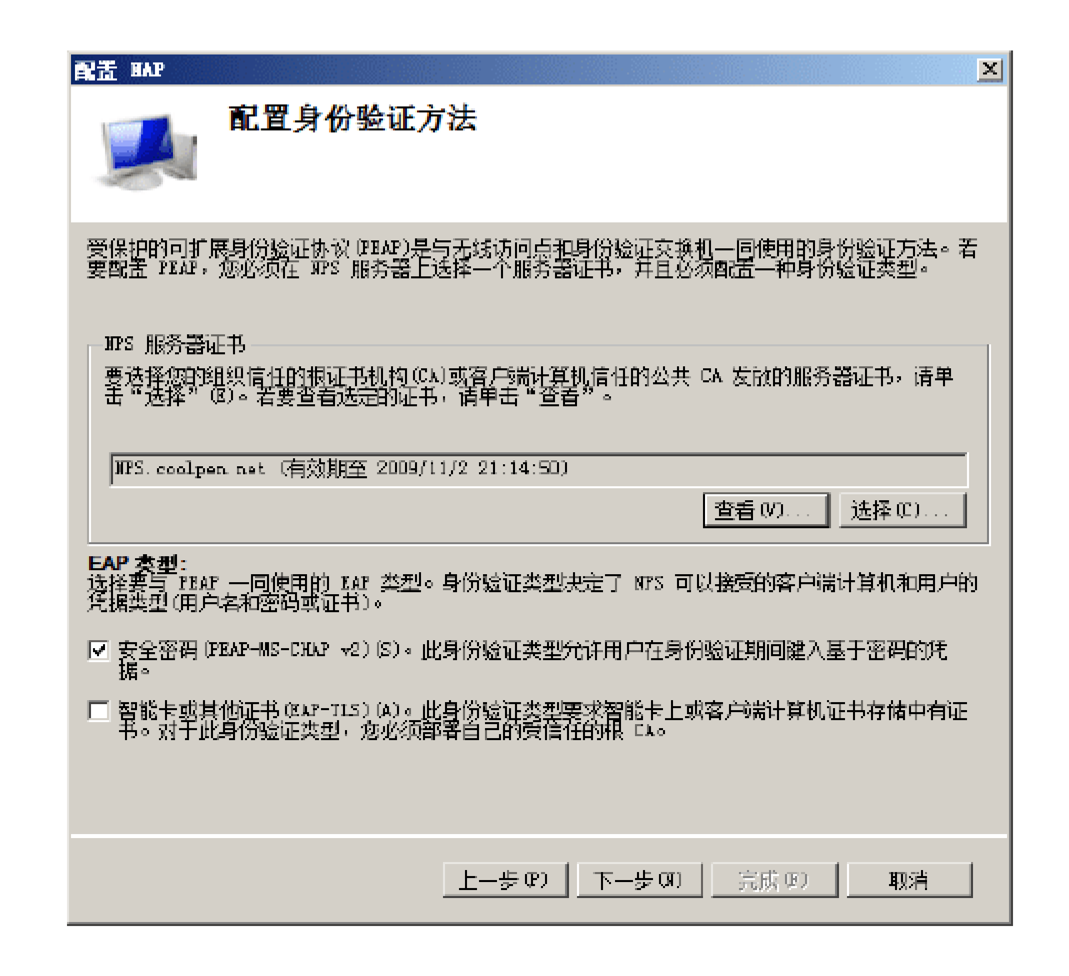


图 14-52　“配置身份验证方法”界面

③　在如图 14-53 所示的“配置虚拟 LAN(VLAN)”界面中，如果 RADIUS 客户端支持 VLAN，则可以配置 NPS 以向 RADIUS 客户端提供包含更新服务器的受限网络，以及提供完全网络访问权限的组织网络的 VLAN 信息。

④　在“配置虚拟 LAN(VLAN)”界面的“组织网络 VLAN”区域中，单击“配置”按钮，显示如图 14-54 所示的“虚拟 LAN(VLAN)配置”对话框。在“RADIUS 标准属性”和“供应商特定属性”选项卡中，配置 802.1X 访问点所需的属性，为符合的 NAP 客户端的内网访问指定 ACL 或 VLAN ID。设置完成后，单击“确定”按钮，保存配置。



图 14-53　“配置虚拟 LAN(VLAN)”界面

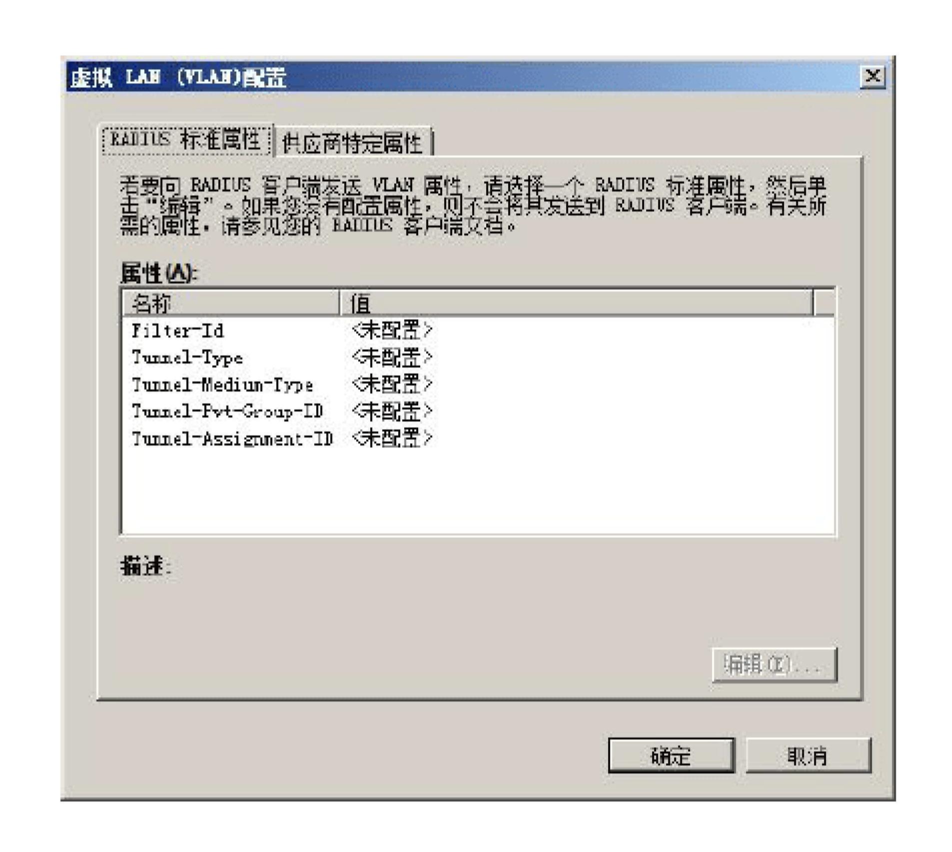


图 14-54　“虚拟 LAN(VLAN)配置”对话框(1)

⑤　在“配置虚拟 LAN(VLAN)”对话框的“受限网络 VLAN”选项区域中，单击“配置”按钮，显示如图 14-55 所示的“虚拟 LAN(VLAN)配置”对话框。在“RADIUS 标准属性”和“供应商特定属性”选项卡中，为内网访问指定 ACL 或 VLAN ID，配置 802.1X 访问点所需的属性。因为想要最初

的 NAP 强制模式为报告模式，所以必须为内网访问配置 ACL 或 VLAN ID，而非受限访问。其他步骤将会为不符合的 NAP 客户端测试受限访问，然后配置强制模式，不符合的 NAP 客户端将会受到访问限制。最后，单击“确定”按钮，保存配置。

(2) 配置常规网络策略设置

① 打开“网络策略服务器”窗口，依次展开“策略”→“网络策略”节点。在右侧栏中，双击无线或有线网络策略，显示策略属性对话框，如图 14-56 所示的“概述”选项卡的“网络连接方法”选项区域中，查看是否设置了“供应商特定”设置，并根据实际情况来选择是否设置。

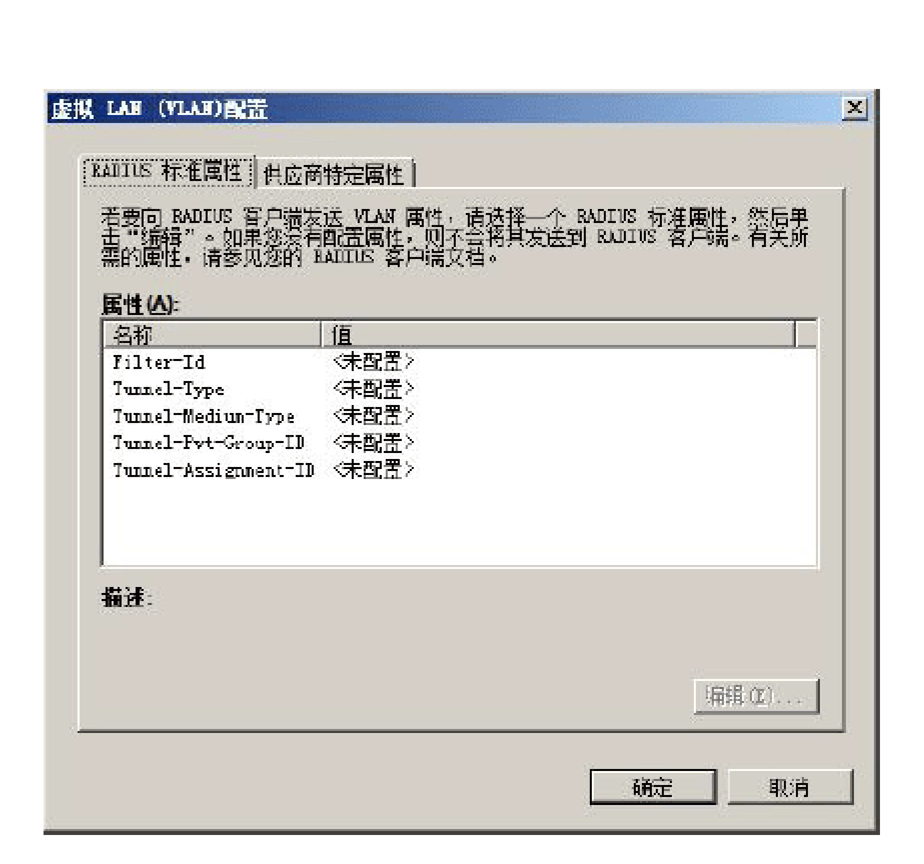


图 14-55 “虚拟 LAN(VLAN)配置”对话框(2)

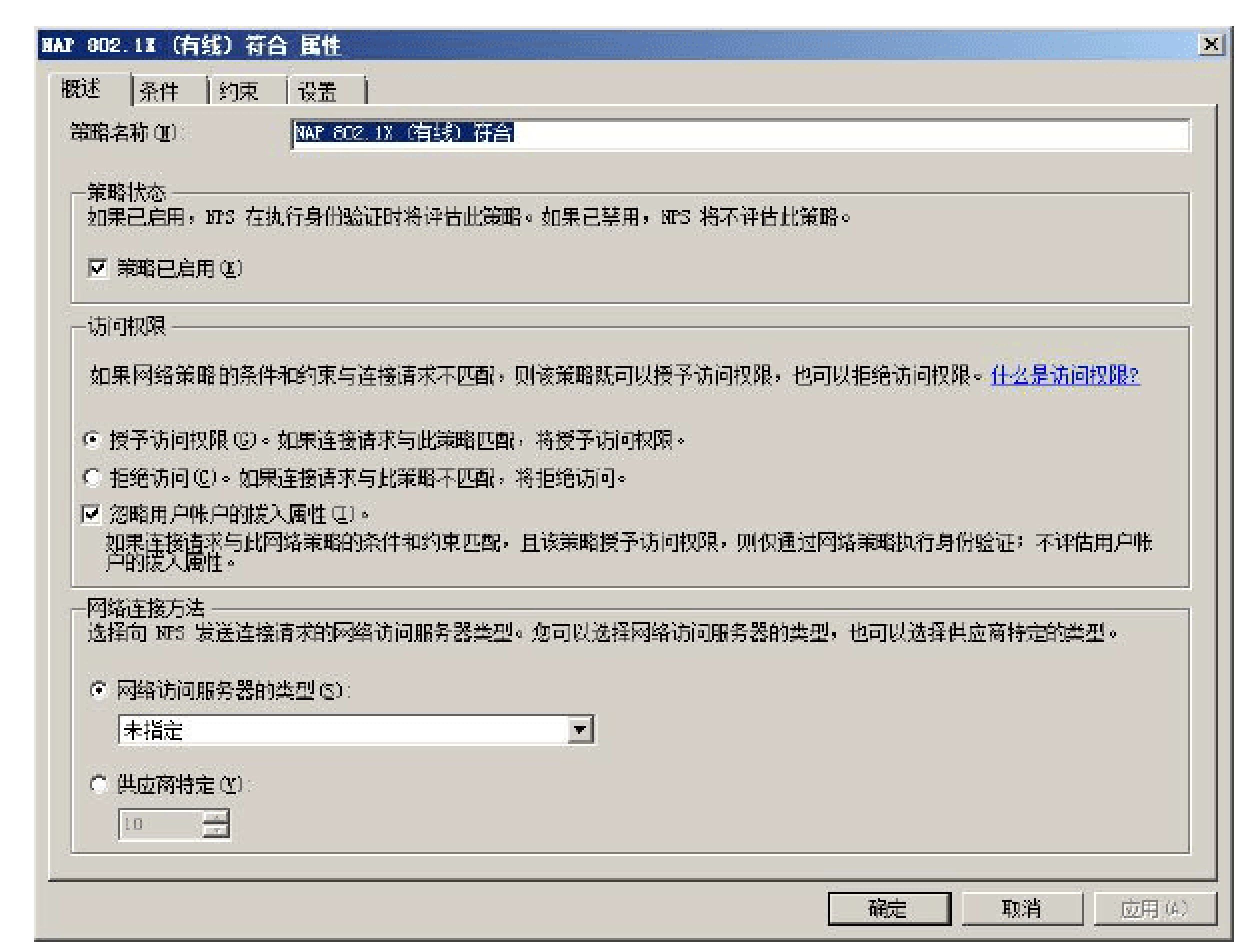


图 14-56 策略属性对话框

② 切换到如图 14-57 所示的“条件”选项卡，查看除了 NAS 端口类型以外是否还有其他条件，并根据实际需要进行设置。

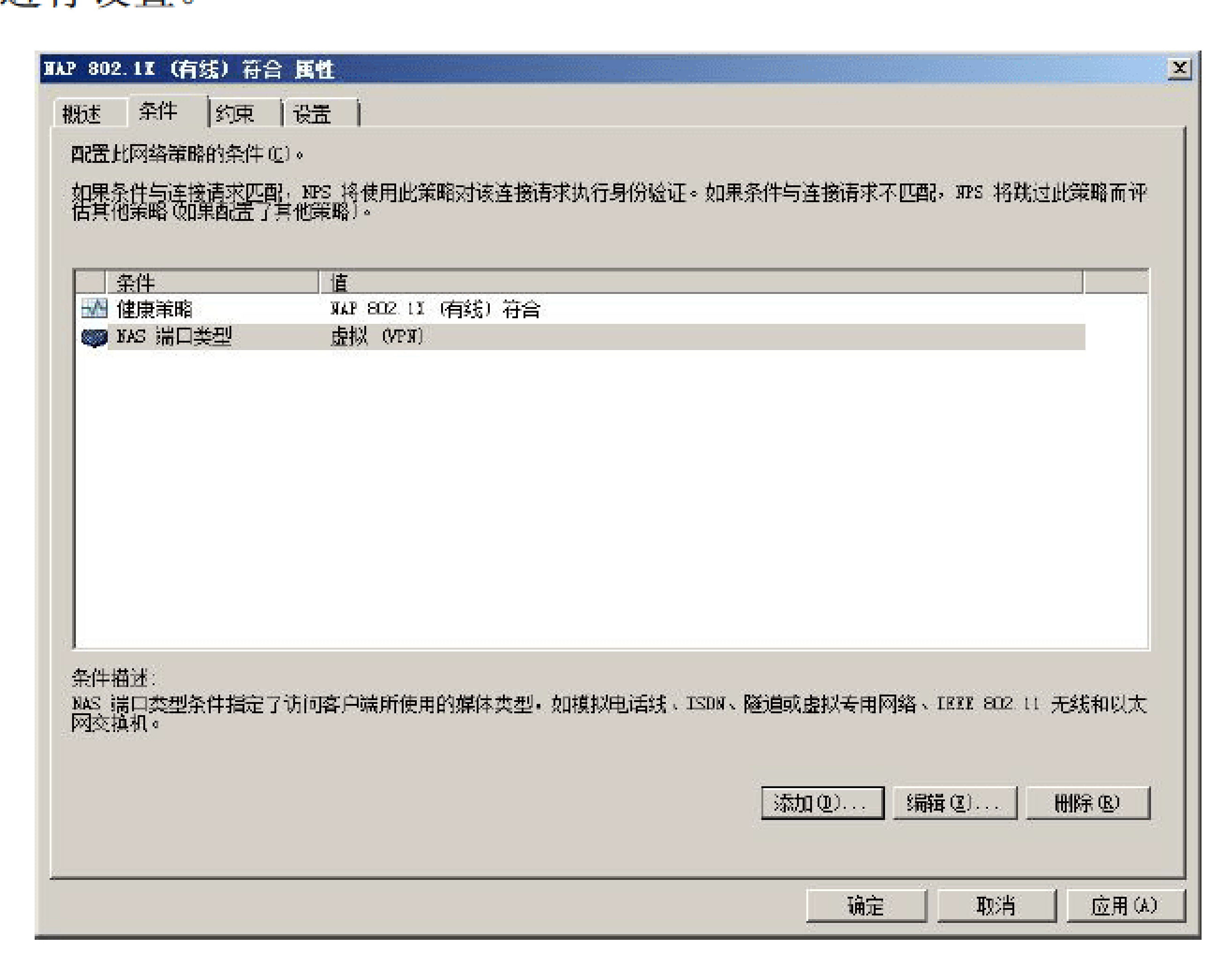


图 14-57 “条件”选项卡

③ 切换到如图 14-58 所示的“约束”选项卡，查看约束列表中的任何设置是否配置了相应值，并根

据实际需要进行设置。

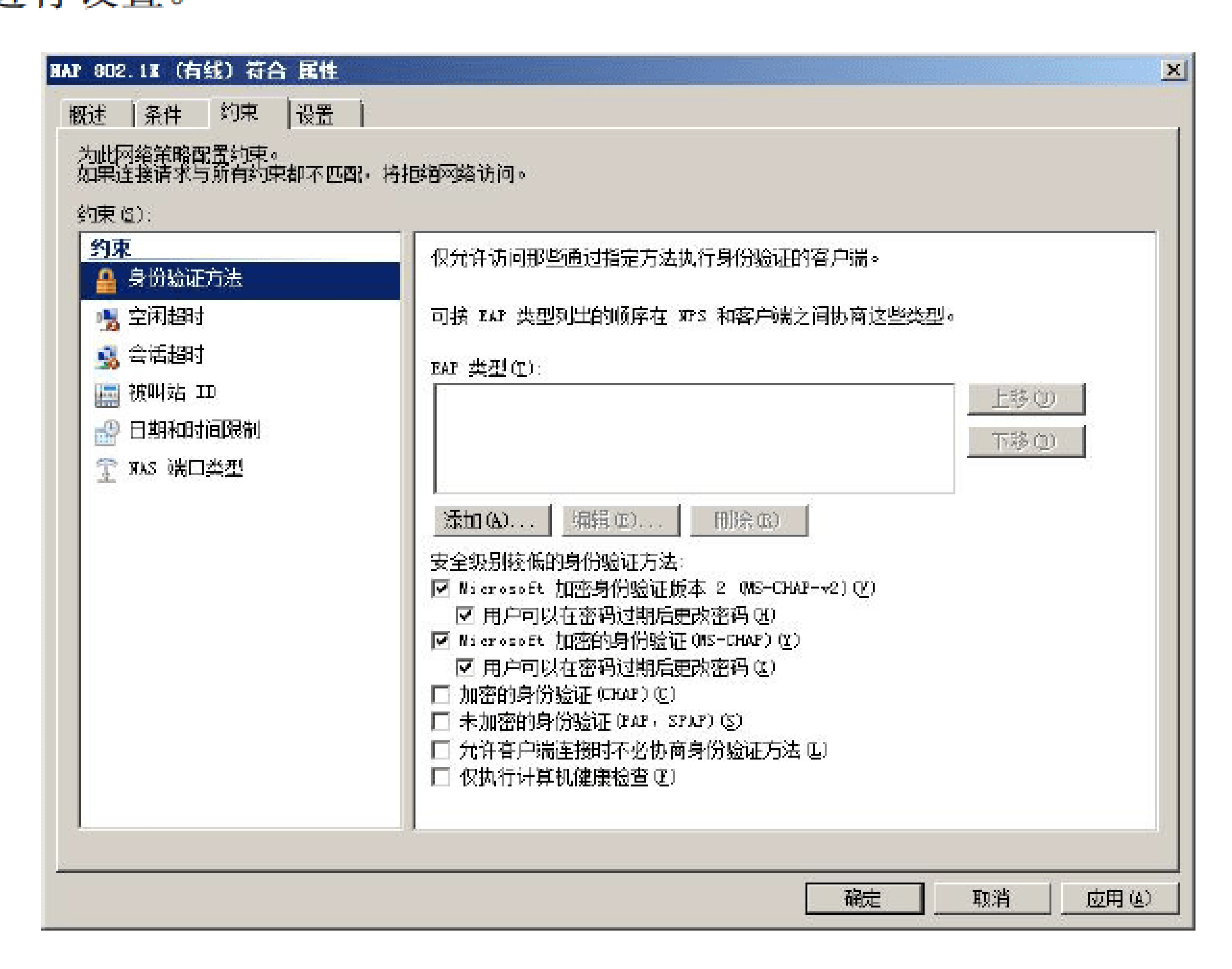


图 14-58 “约束”选项卡

④ 切换到如图 14-59 所示的“设置”选项卡，查看任意其他 RADIUS 标准或供应商指定属性是否配置了 Framed-Protocol 和 Service-Type，并根据实际需要进行设置。

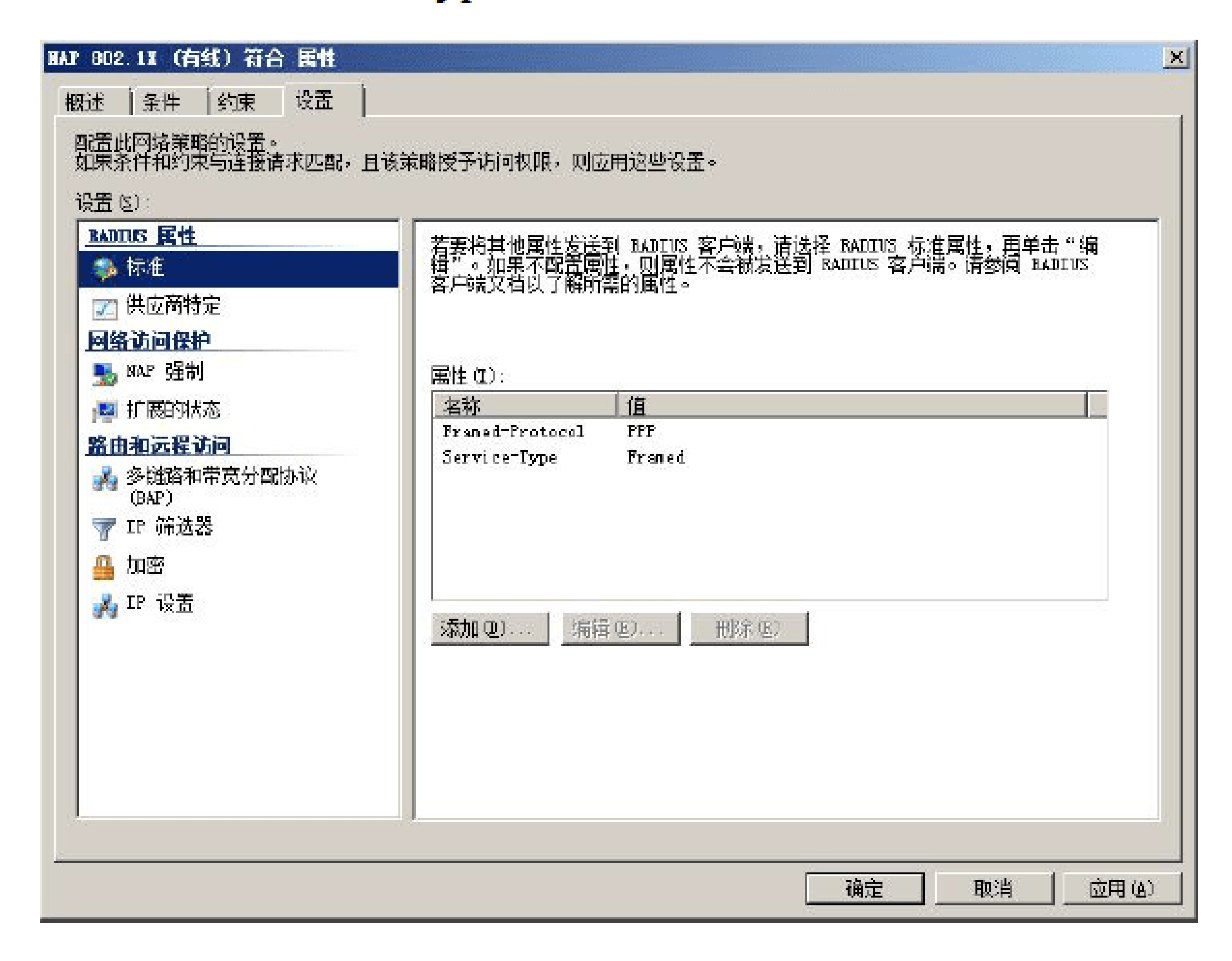


图 14-59 “设置”选项卡

⑤ 连续单击“确定”按钮，保存设置。

⑥ 双击“配置 NAP 向导”为符合的 NAP 客户端创建无线或有线网络策略。在“概述”、“条件”、“约束”和“设置”选项卡中，根据第①步～第⑤步确定的网络策略配置现有无线或有线策略的设置。

⑦ 双击“配置 NAP 向导”为不符合的 NAP 客户端创建无线或有线网络策略。在“概述”、“条件”、“约束”和“设置”选项卡中，根据第①步～第⑤步确定的网络策略配置现有无线或有线策略的设置。

⑧ 双击“配置 NAP 向导”为不具有 NAP 功能客户端创建无线或有线网络策略。在“概述”、“条

件”、“约束”和“设置”选项卡中，根据第②步～第⑤步确定的网络策略配置现有无线或有线策略的设置。

(3) 配置报告模式

① 打开“网络策略服务器”管理单元中，依次展开“策略”→“网络策略”节点。在右侧栏中，双击“配置 NAP 向导”创建的不符合的 NAP 客户端的网络策略。

② 切换到“设置”选项卡，然后单击“NAP 强制”选项，显示如图 14-60 所示的“NAP 802.1X(有线)不符合 属性”对话框。在网络策略属性对话框的详细面板中，选择“允许完全网络访问”单选按钮。

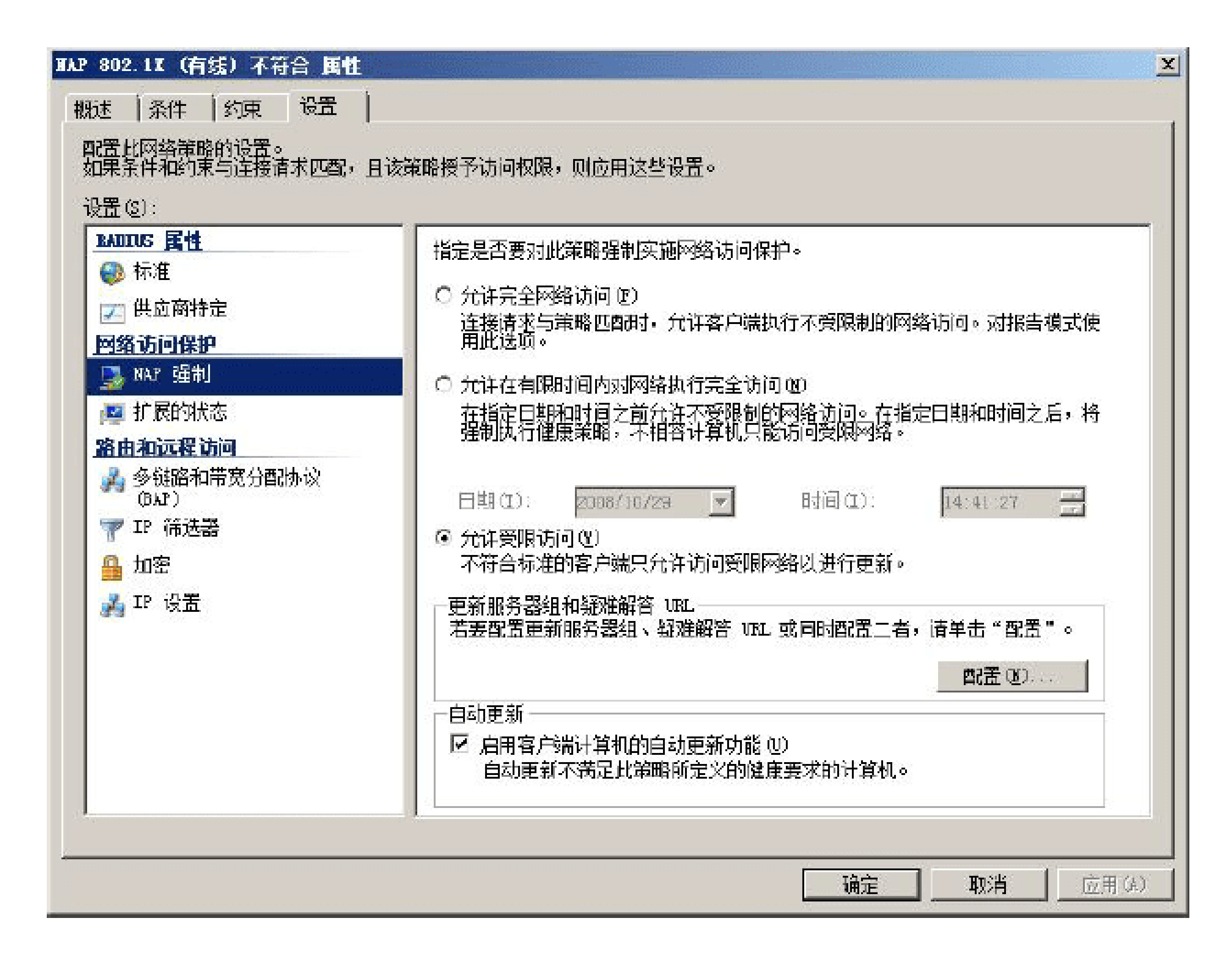


图 14-60 “NAP 802.1X(有线)不符合 属性”对话框

③ 单击“确定”按钮，保存设置。

(4) 为所要求的健康设置配置健康策略条件

① 在“网络策略服务器”管理单元中，依次展开“策略”→“健康策略”节点。

② 双击符合和不符合的 NAP 客户端的健康策略，根据健康评估条件和 SHV 的需要进行设置。

在该配置中，创建并配置了 NAP 健康要求策略，但是 NAP 健康策略服务器仍然使用已有的无线或有线连接要求，以及无线或有线访问的网络策略。因此，必须修改连接请求策略的配置，确保 802.1X 强制的新的连接请求策略用于有线或无线连接。

(5) 为 802.1X 强制修改连接请求策略

“配置 NAP 向导”创建的无线或有线连接的连接请求策略，要求使用基于 PEAP 的身份验证方法，以及系统健康检查。不使用基于 PEAP 的身份验证方法的 802.1X 客户端的连接尝试，将会被 NAP 健康策略服务器拒绝。使用基于 PEAP 的身份验证方法，但是不符合健康状态要求的 NAP 客户端，将被 NAP 健康策略服务器定义为不具有 NAP 功能的客户端。

14.2.4 配置 NAP 客户端

尽管可以单独配置 NAP 客户端，但是在活动目录域环境下集中配置 NAP 客户端的最好方法就是通过

组策略设置，主要包括如下步骤。

① 为 PEAP 启用系统健康检查。

② 配置 NAP 客户端设置。

③ 启用 Windows 安全中心(请参考 IPSec NAP 客户端的配置)。

④ 配置网络访问保护代理服务的自动启用(请参考 IPSec NAP 客户端的配置)。

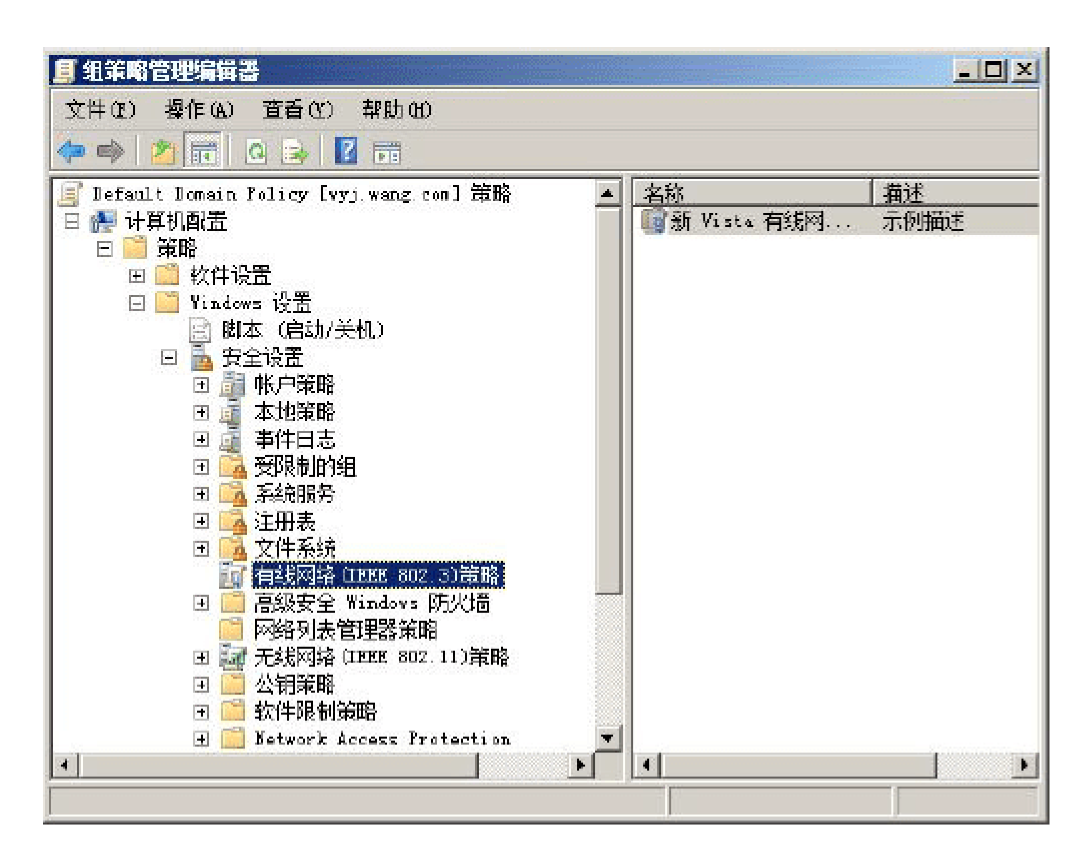
1. 为 PEAP 启用系统健康检查

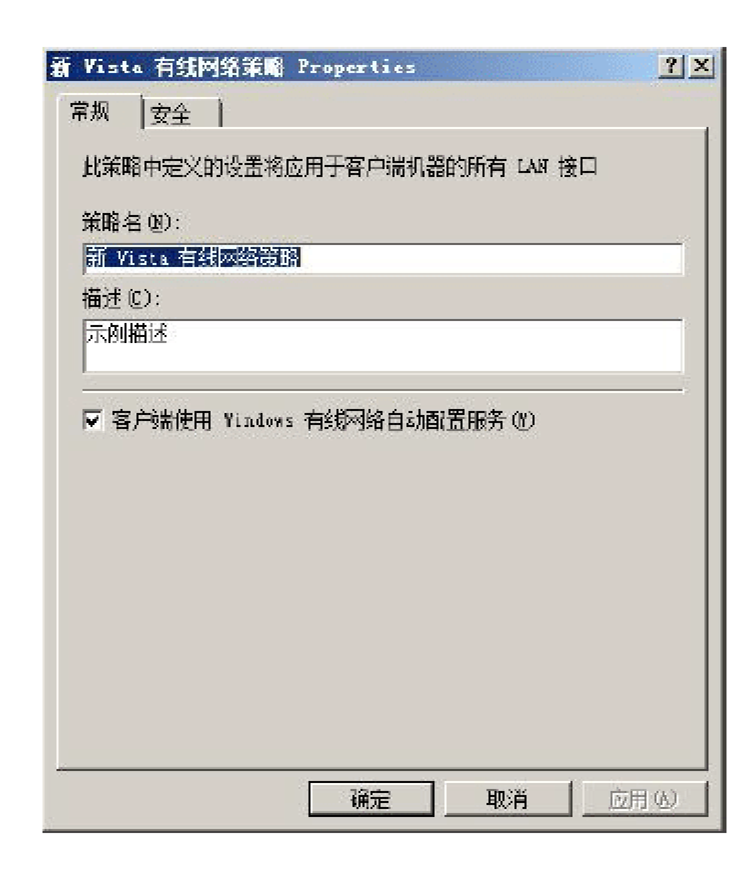
尽管已经配置了 NAP 客户端使用 PEAP 身份验证协议，但是如果 PEAP 身份验证协议不启用系统健康检查， NAP 客户端将不会回应系统健康状态的请求。通过组策略扩展，可以为有线和无线网络启用 PEAP 的系统健康检查。

2. 在组策略中为 PEAP 启用系统健康检查

① 打开“组策略管理”窗口，右击想要设置的策略名称，在弹出的快捷菜单中选择“编辑”命令，打开如图 14-61 所示的“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“有线网络(IEEE 802.3)策略”。

② 双击有线网络策略，显示如图 14-62 所示的有线网络策略属性对话框。在“策略名”和“描述”文本框中，可根据需要设置策略名称和描述信息。





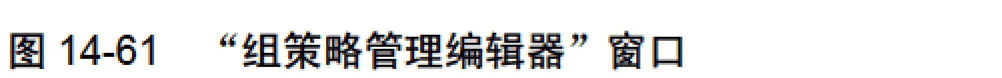


图 14-61　“组策略管理编辑器”窗口　　　图 14-62　有线网络策略属性对话框

③ 切换至如图 14-63 所示的“安全”选项卡，单击“属性”按钮，显示如图 14-64 所示的“受保护的 EAP 属性”对话框，选中“启用隔离检查”复选框。

④ 连续单击“确定”按钮，返回到“组策略管理编辑器”窗口。

⑤ 对于无线连接，在控制台中，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“无线网络(IEEE 802.11)策略”节点，如图 14-65 所示。

⑥ 双击 Vista 无线连接策略，显示如图 14-66 所示的“Vista 无线连接策略 属性”对话框。双击相应的无线配置文件，显示如图 14-67 所示的“新建配置文件(1) 属性”对话框。根据实际需要，设置配置文件的连接信息。

⑦ 切换至“安全”选项卡，单击“属性”按钮，显示如图 14-68 所示的“受保护的 EAP 属性”对话框，选中“启用隔离检查”复选框。

⑧ 连续单击“确定”按钮，返回到“组策略管理编辑器”对话框。

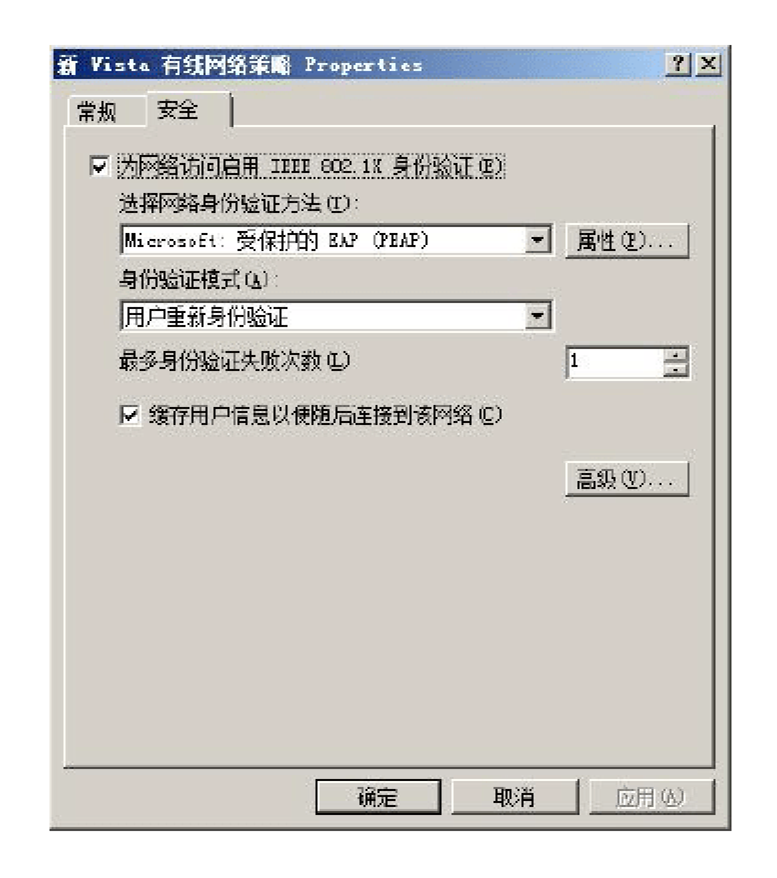


图 14-63 “安全”选项卡



图 14-64 “受保护的 EAP 属性”对话框

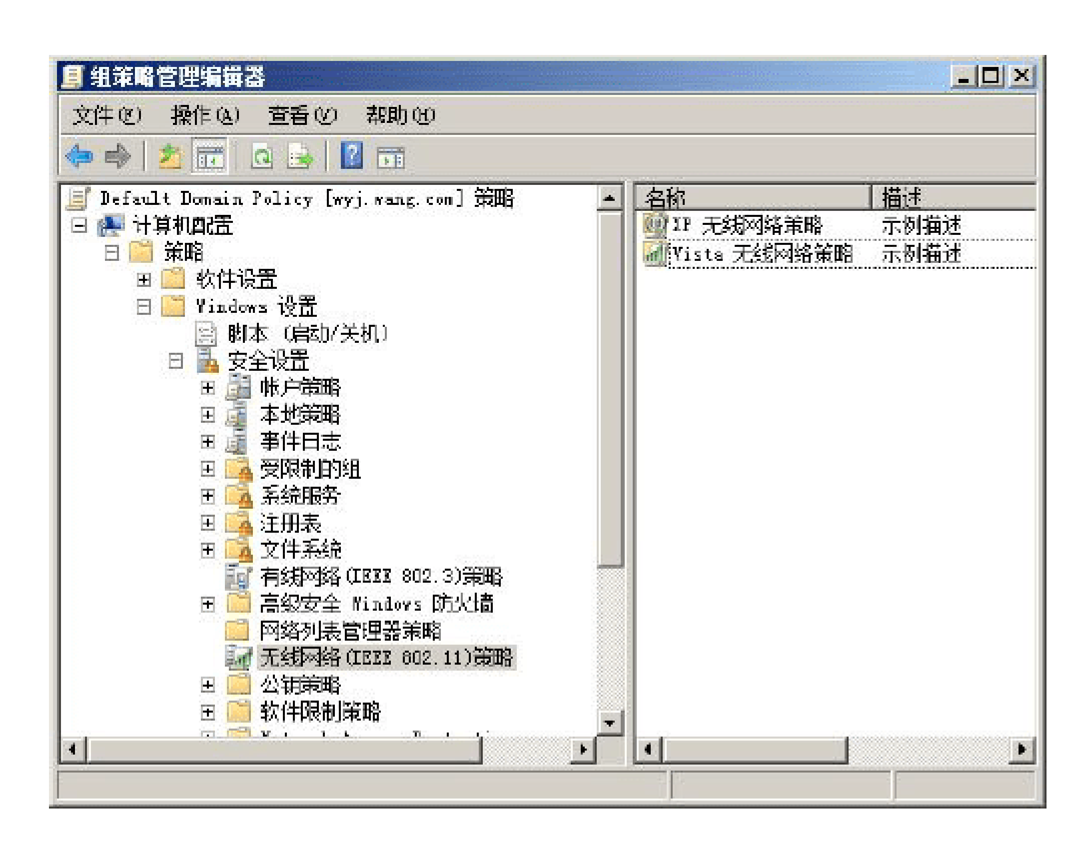


图 14-65 展开“无线网络(IEEE 802.11)策略”

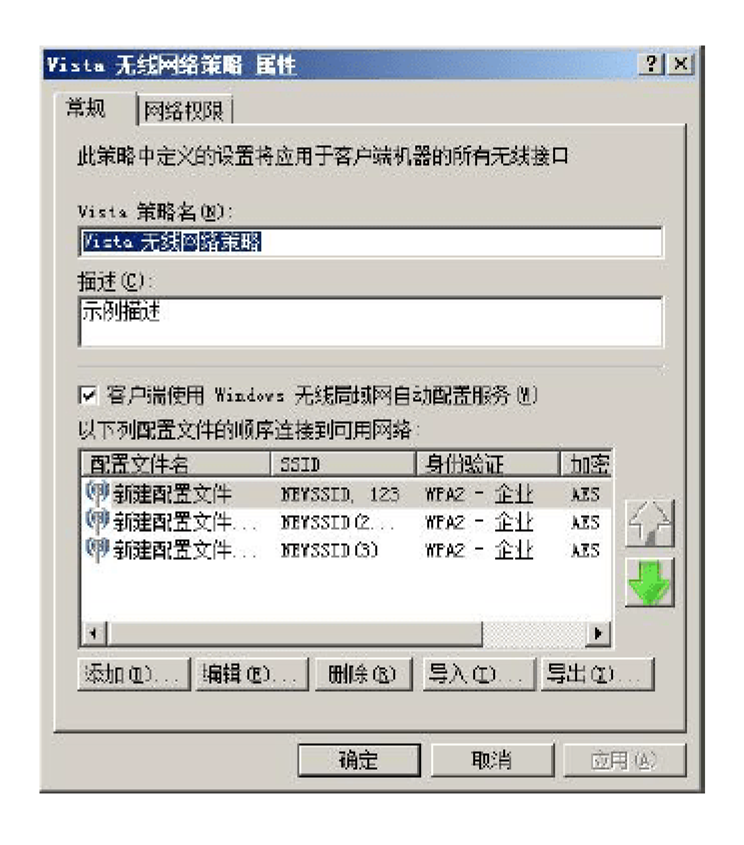


图 14-66 “Vista 无线网络策略 属性”对话框

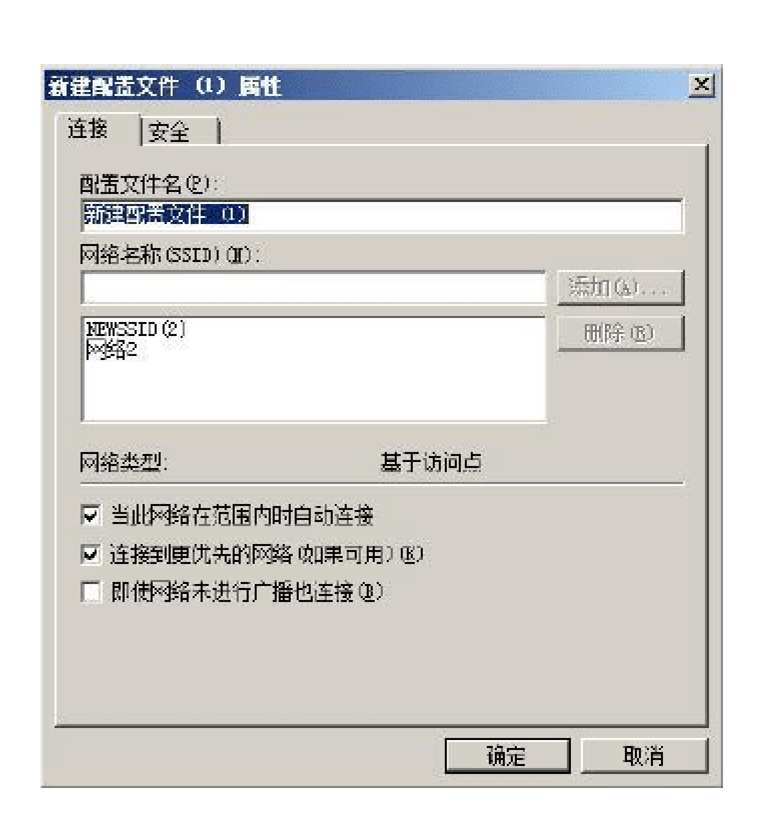


图 14-67 “新建配置文件 (1) 属性”对话框

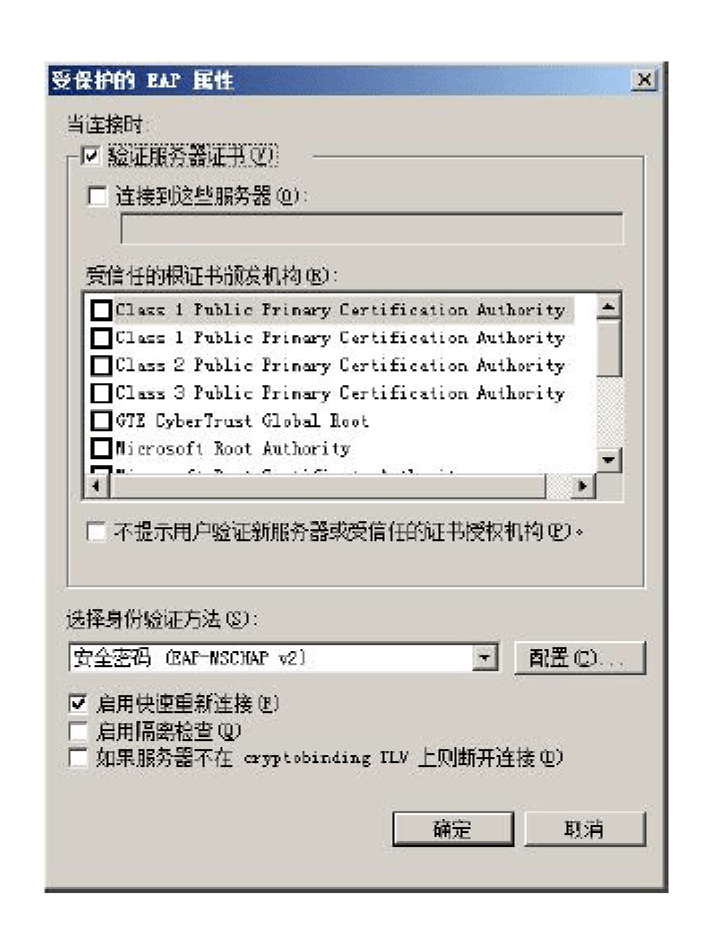


图 14-68 “受保护的 EAP 属性”对话框

⑨　双击“XP 无线网络策略”，显示如图 14-69 所示的“XP 无线网络策略 属性”对话框。根据需要，设置无线网络策略的名称和描述信息。

⑩　切换至如图 14-70 所示的“首选网络”选项卡，在“网络”列表框中，双击相应的无线网络名称，显示如图 14-71 所示的“编辑 NEWSSID 属性”对话框，即可开始编辑其属性设置。

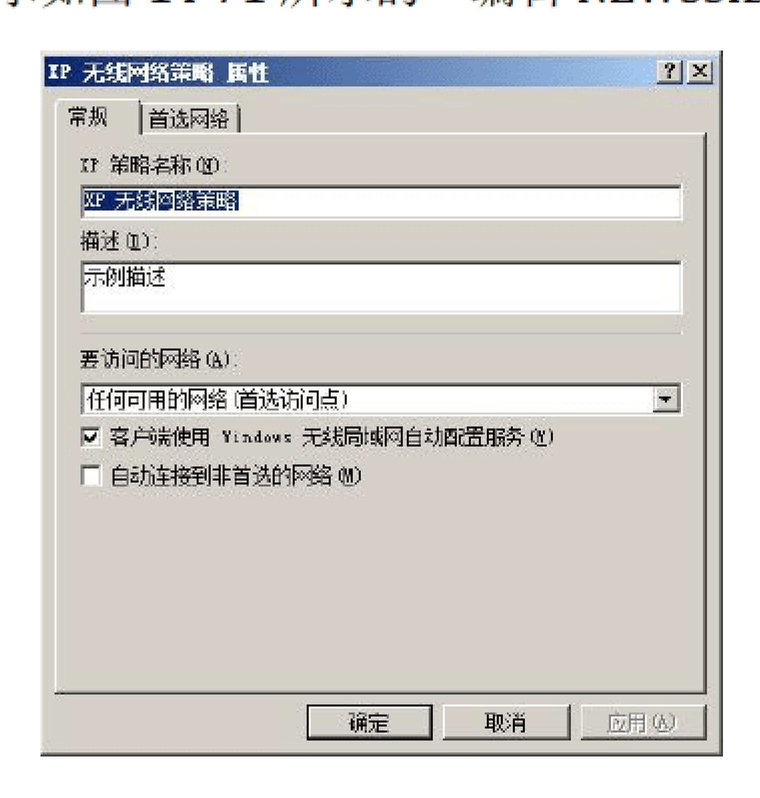


图 14-69　“XP 无线网络策略 属性”对话框



图 14-70　“首选网络”选项卡

⑪　切换到如图 14-72 所示的 IEEE 802.1X 选项卡，单击“设置”按钮，显示如图 14-73 所示的“受保护的 EAP 属性”对话框，选中“启用隔离检查”复选框。

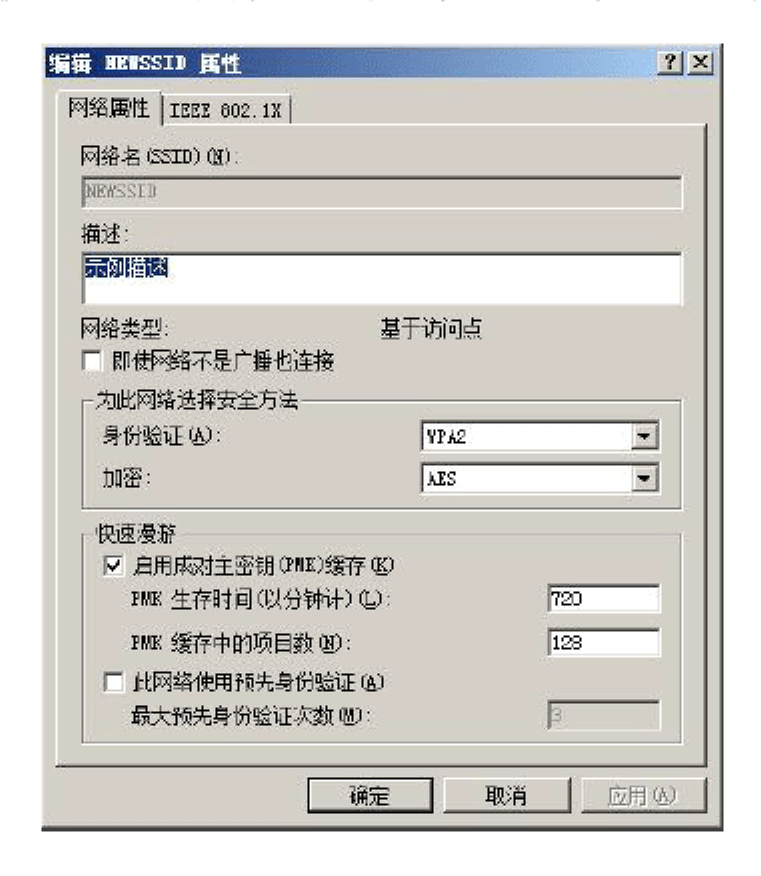


图 14-71　“编辑 NEWSSID 属性”对话框

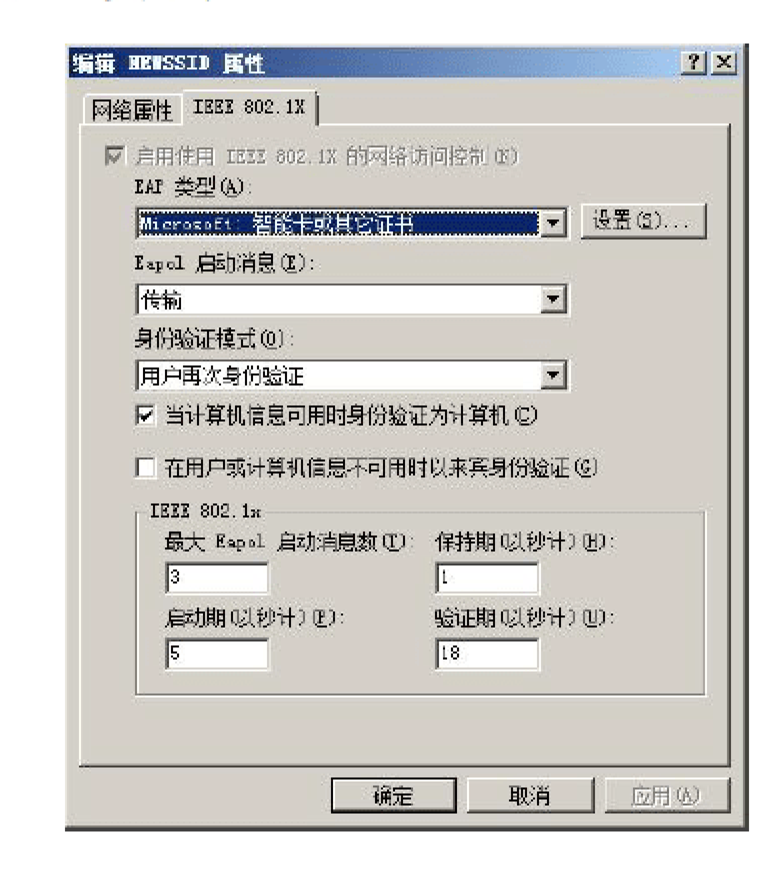


图 14-72　IEEE 802.1X 选项卡

⑫　连续单击“确定”按钮，返回到“组策略管理编辑器”对话框。



提示：因为在运行 Windows XP 的计算机上，没有组策略为有线网络配置 802.1X 身份验证属性，所以必须手动启用 PEAP 的系统健康检查。

3. 配置 NAP 客户端设置

打开“组策略管理”窗口。依次展开“林”→“域”节点，在“链接的组策略对象”面板中，右击适当的组策略对象，在弹出的快捷菜单中选择“编辑”命令，打开“组策略管理编辑器”窗口。依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“网络访问保护”→“NAP 客户端配置”节点。

在控制台中，单击“强制客户端”，在右侧栏中，双击“EAP 隔离强制客户端”图标，显示如图 14-74 所示的“EAP 隔离强制客户端 属性”对话框。选中“启用此强制客户端”复选框，单击“确定”按钮，保存设置。

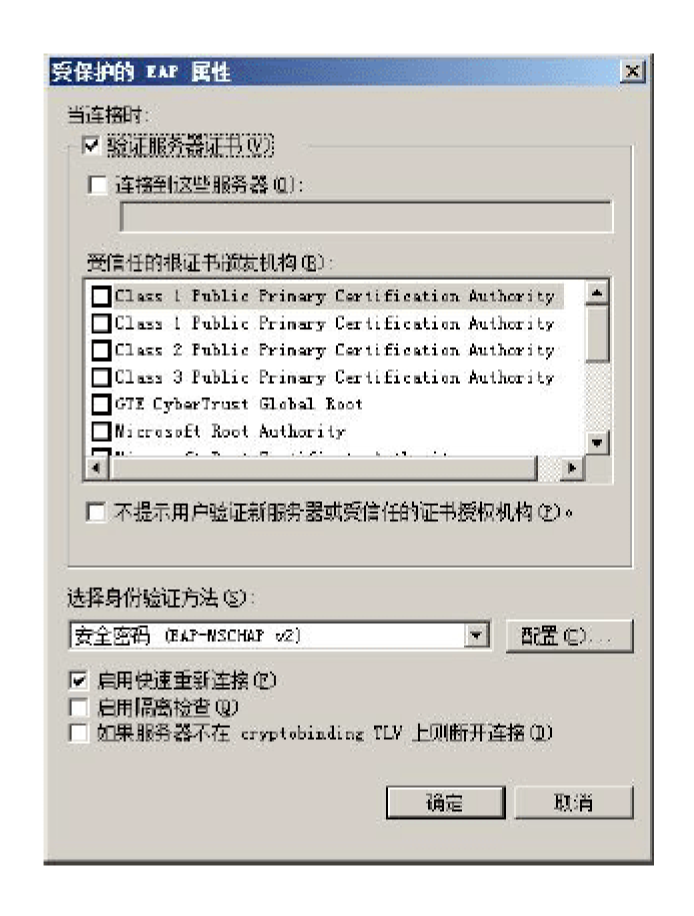


图 14-73 “受保护的 EAP 属性”对话框

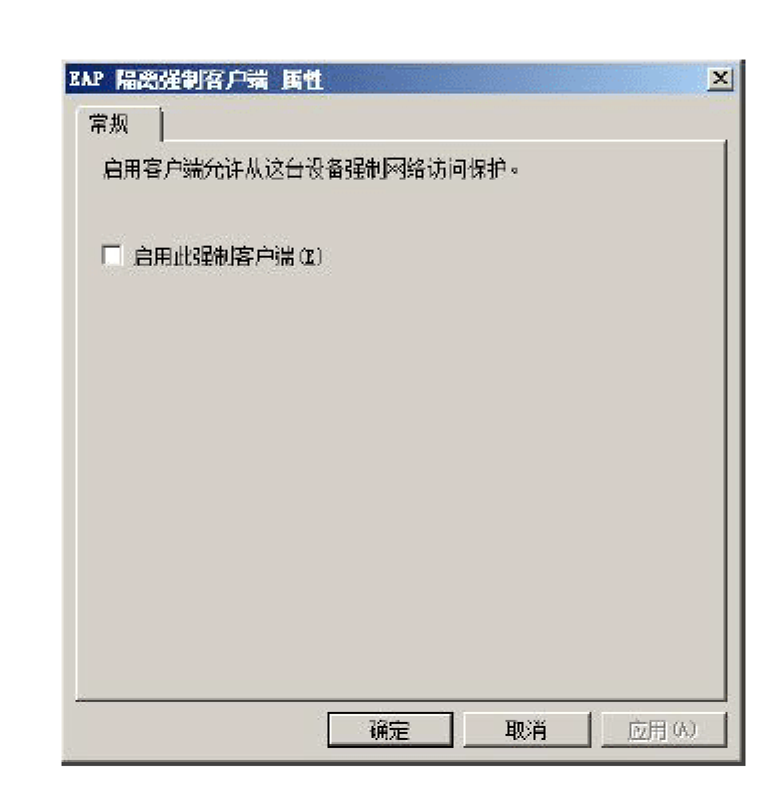


图 14-74 “EAP 隔离强制客户端 属性”对话框

对于运行 Windows XP SP3 的计算机，在控制台中，依次展开“计算机配置”→“管理模板”→“Windows 组件”→“网络访问保护”节点。然后在右侧栏中，双击“允许网络访问保护客户端支持 802.1X 强制客户端组件”图标，显示如图 14-75 所示的“允许网络访问保护客户端支持 802.1x 强制客户端组件 属性”对话框。在“设置”选项卡中，选择“已启用”单选按钮，然后单击“确定”按钮，保存设置即可。

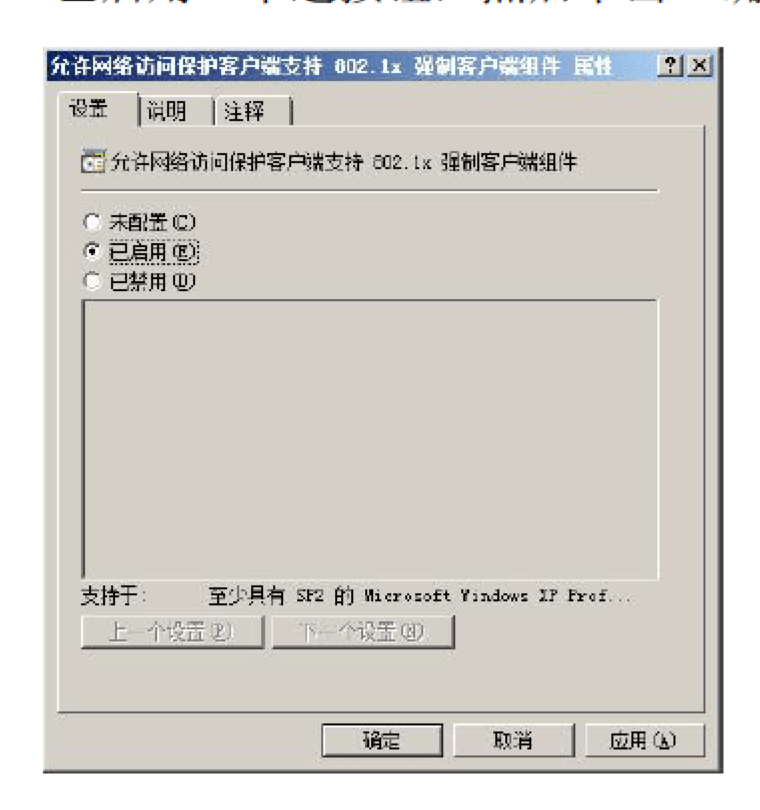


图 14-75 “允许网络访问保护客户端支持 802.1x 强制客户端组件 属性”对话框

14.2.5 测试受限访问

在启用强制模式前，必须测试不符合的 NAP 客户端的连接是否被分配了正确 ACL 或 VLAN ID。具体测试步骤如下。

① 为安全组成员的 NAP 客户端的受限访问创建新的网络策略。

② 确保不符合的访问受限的测试计算机配置了相应的 ACL 或 VLAN ID，并且只能访问内网的更新服务器。

1. 为测试组创建新的网络策略

① 指定内网中的一些计算机作为受限访问的测试计算机。

② 使用“活动目录用户和计算机”管理单元，为测试受限访问创建一个安全组，并且将指定的计算机添加到该组中。

③ 在“网络策略服务器”管理单元中，依次展开“策略”→“网络策略”节点。

④ 右击使用“配置 NAP 向导”创建的不符合的 NAP 客户端的无线或有线网络策略，在弹出的快捷菜单中选择“重复策略”选项，创建策略副本，如图 14-76 所示。

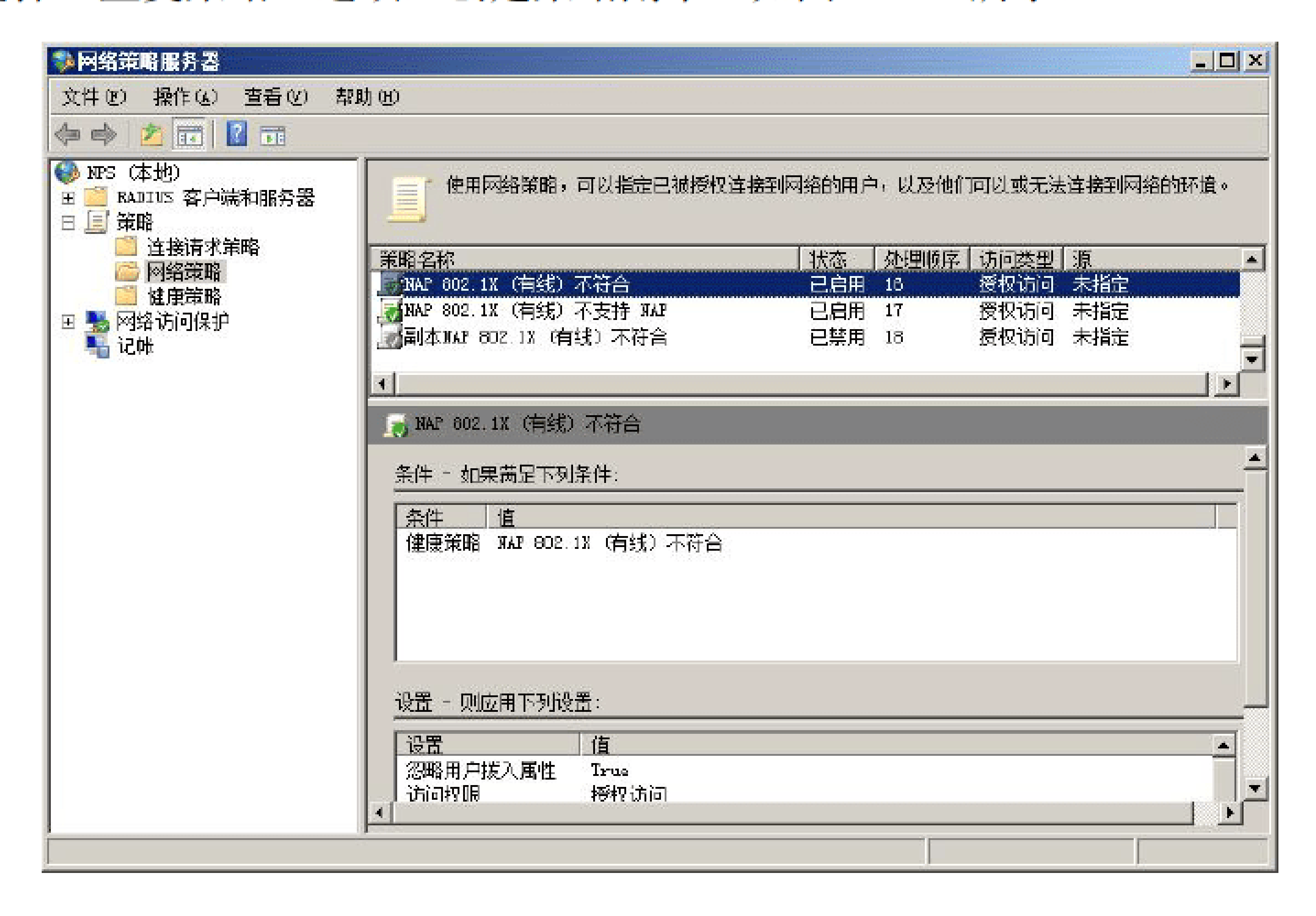


图 14-76　网络策略副本

⑤ 双击不符合的 NAP 客户端的无线或有线网络策略的副本，显示如图 14-77 所示的“副本 NAP 802.1X (有线)不符合 属性”对话框。在“策略名称”文本框中，输入新的网络策略的名称。在“策略状态”区域中，选中“策略已启用”复选框。

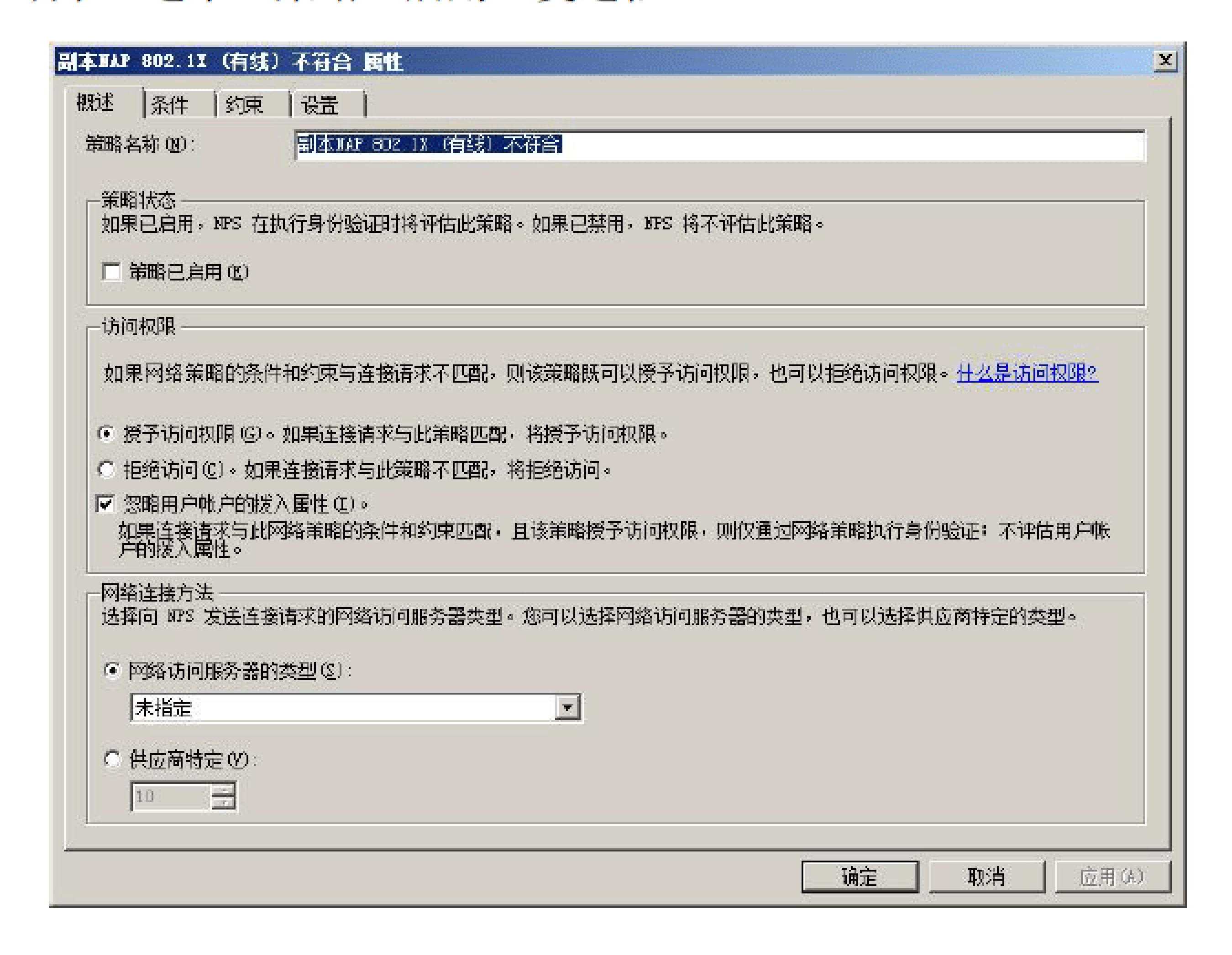


图 14-77　“副本 NAP 802.1X (有线)不符合 属性”对话框

⑥ 切换到“条件”选项卡，单击“添加”按钮，显示如图 14-78 所示的“选择条件”对话框。

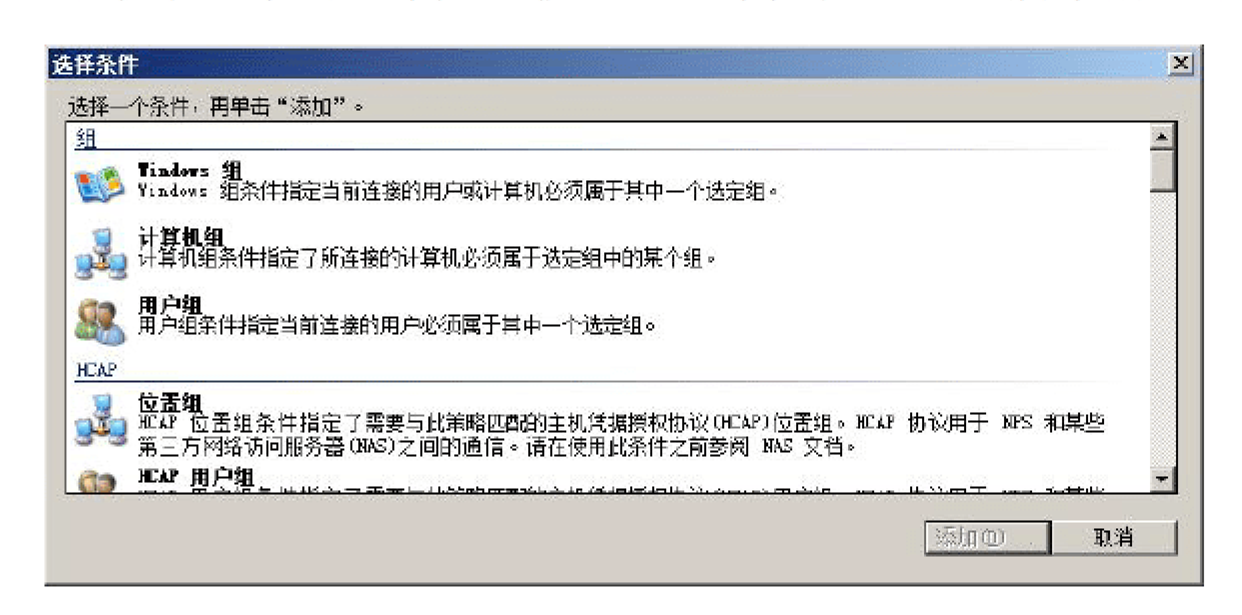


图 14-78 “选择条件”对话框

⑦ 双击“Windows 组”选项，显示“Windows 组”对话框。单击“添加组”按钮，显示“选择组”对话框，指定预先创建的组名称，然后单击两次“确定”按钮，返回到“副本 NAP 802.1X (有线) 不符合 属性”对话框。

⑧ 切换到“设置”选项卡，在“RADIUS 属性”区域，单击“标准”选项，如图 14-79 所示。修改 RADIUS 标准属性，为受限访问指定 ACL 或 VLAN ID。

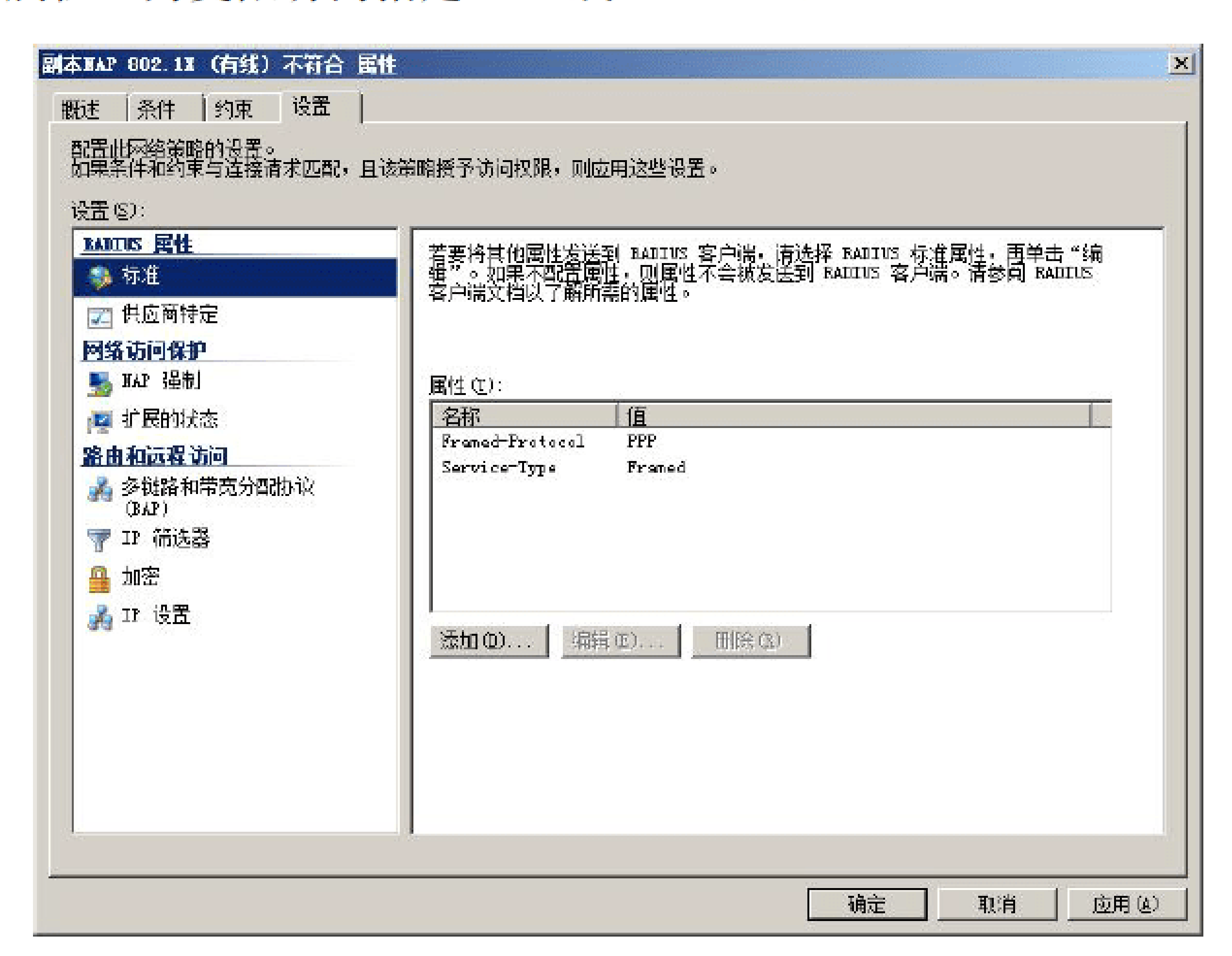


图 14-79 RADIUS 标准设置

⑨ 在“RADIUS 属性”区域中，单击“供应商特定”选项，如图 14-80 所示。根据实际需要，修改供应商特定属性为受限访问指定 ACL 或 VLAN ID。

⑩ 在“网络访问保护”区域中，单击“NAP 强制”选项，如图 14-81 所示。在右侧栏中，选择“允许受限访问”单选按钮，并取消选中“启用客户端计算机的自动更新功能”复选框。

⑪ 单击“配置”按钮，显示如图 14-82 所示的“更新服务器和疑难解答 URL”对话框。在“疑难解答 URL”文本框中，输入疑难解答 URL 更新服务器的页面 URL。

⑫ 单击两次“确定”按钮，保存设置。

⑬ 右击不符合的 NAP 客户端的网络策略副本，在弹出的快捷菜单中选择“上移”命令，将策略副本上移。重复操作，直至不符合的 NAP 客户端的网络策略副本位于不符合的 NAP 客户端的网络策略之上。

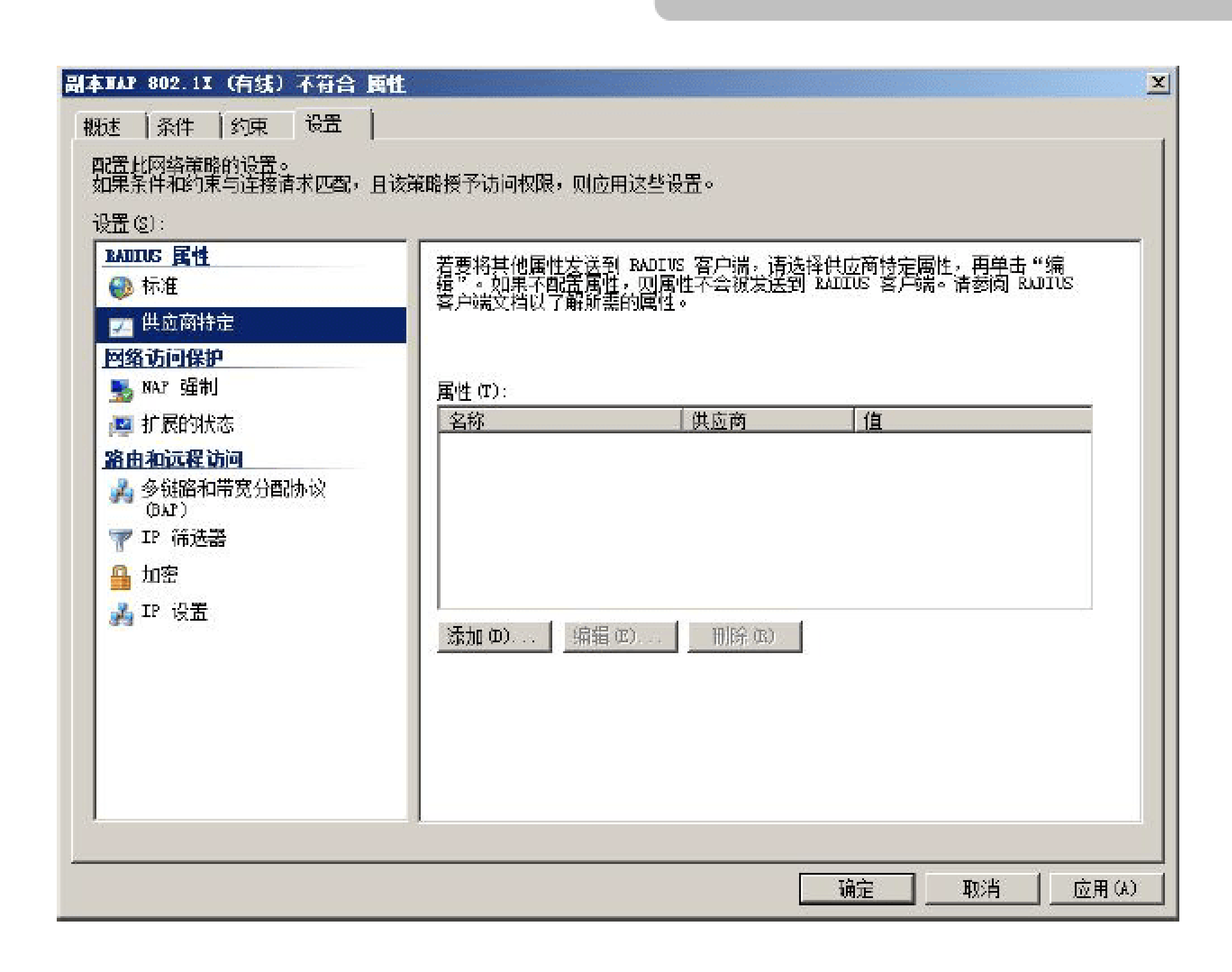


图 14-80　供应商特定设置

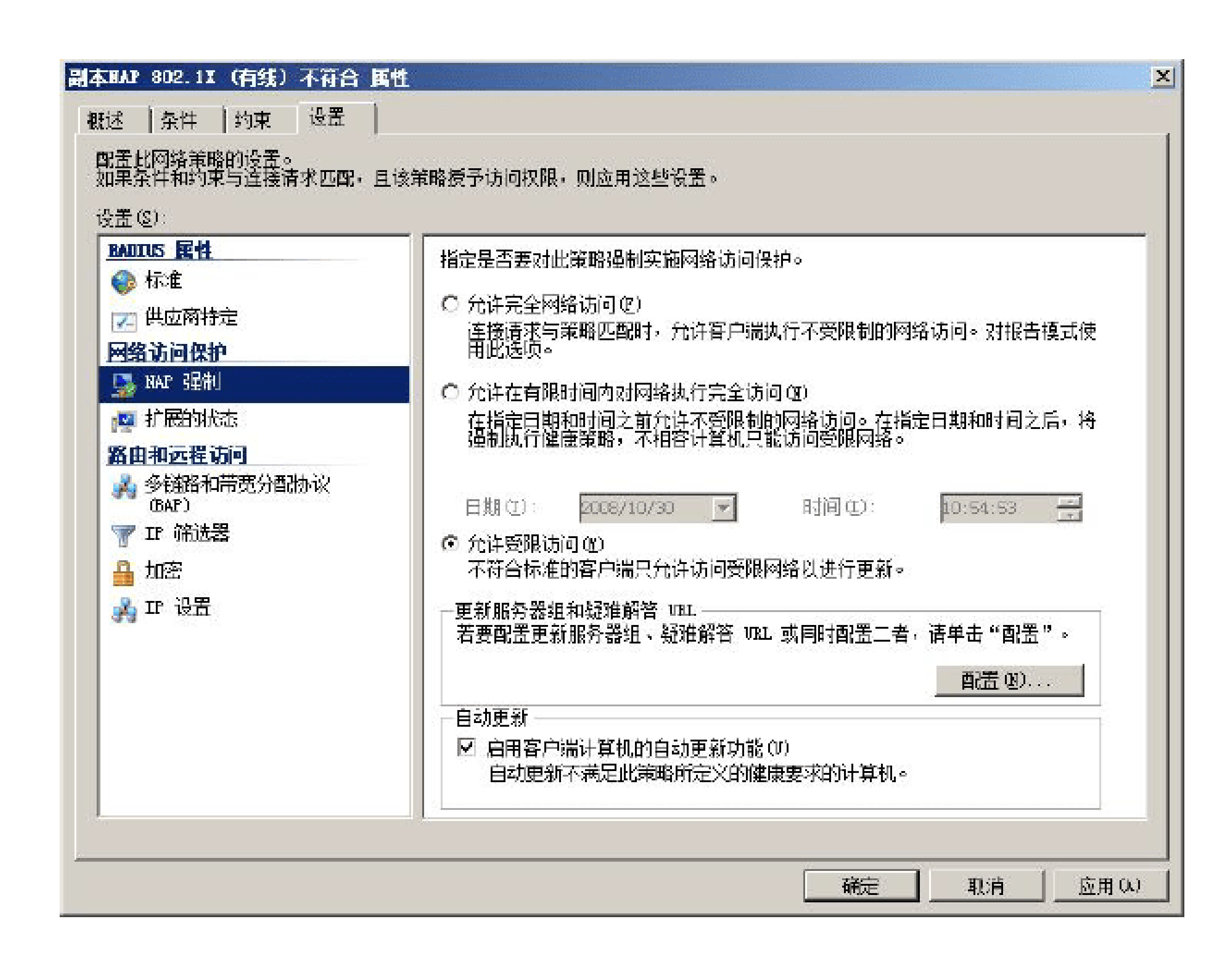


图 14-81　“NAP 强制”配置

图 14-82　“更新服务器和疑难解答 URL”对话框

2. 为不符合的测试计算机测试受限访问

① 为了测试受限访问，将安全组中的测试计算机配置为不符合。根据系统健康要求，可能需要手动禁用自动更新或 Windows 防火墙。

② 在网络连接文件夹中，通过禁用然后启用无线或有线网络适配器来强制 802.1X 身份验证。

③ 当 802.1X 身份验证完成时，应该会看到网络访问保护的通知消息。也可以通过运行命令 ipconfig /all 验证受限状态。

④ 验证是否可以到达所有更新服务器，并能访问疑难解答 URL。

⑤ 验证内网中除了更新服务器，不能到达其他服务器。

根据测试，为不符合的 NAP 客户端修改网络策略的副本，如更新服务器组、疑难解答 URL、RADIUS 属性，或者 802.1X 访问点的 ACL 或 VLAN 受限网络配置。在更新服务器上，可以使用系统健康要求的软件

和 SHA 安装软件，确保软件和 SHA 安装软件安装在不符合的 NAP 客户端上。

14.2.6 为不符合的 NAP 客户端的延期强制配置网络策略

在为不符合的 NAP 客户端测试完网络通信后，确定延期强制模式的日期。到达该日期，不符合的 NAP 客户端将会被置于受限网络中。在 802.1X 强制的延期强制模式下，不符合的 NAP 客户端仍置于内网中，但是用户会收到通知消息，通知其计算机不符合系统健康要求。

打开网络策略属性对话框，切换到“设置”选项卡，然后单击“NAP 强制”选项，如图 14-83 所示。选择“允许在有限时间内对网络执行完全访问”单选按钮，指定 NAP 健康策略服务器上配置的日期和时间即可。

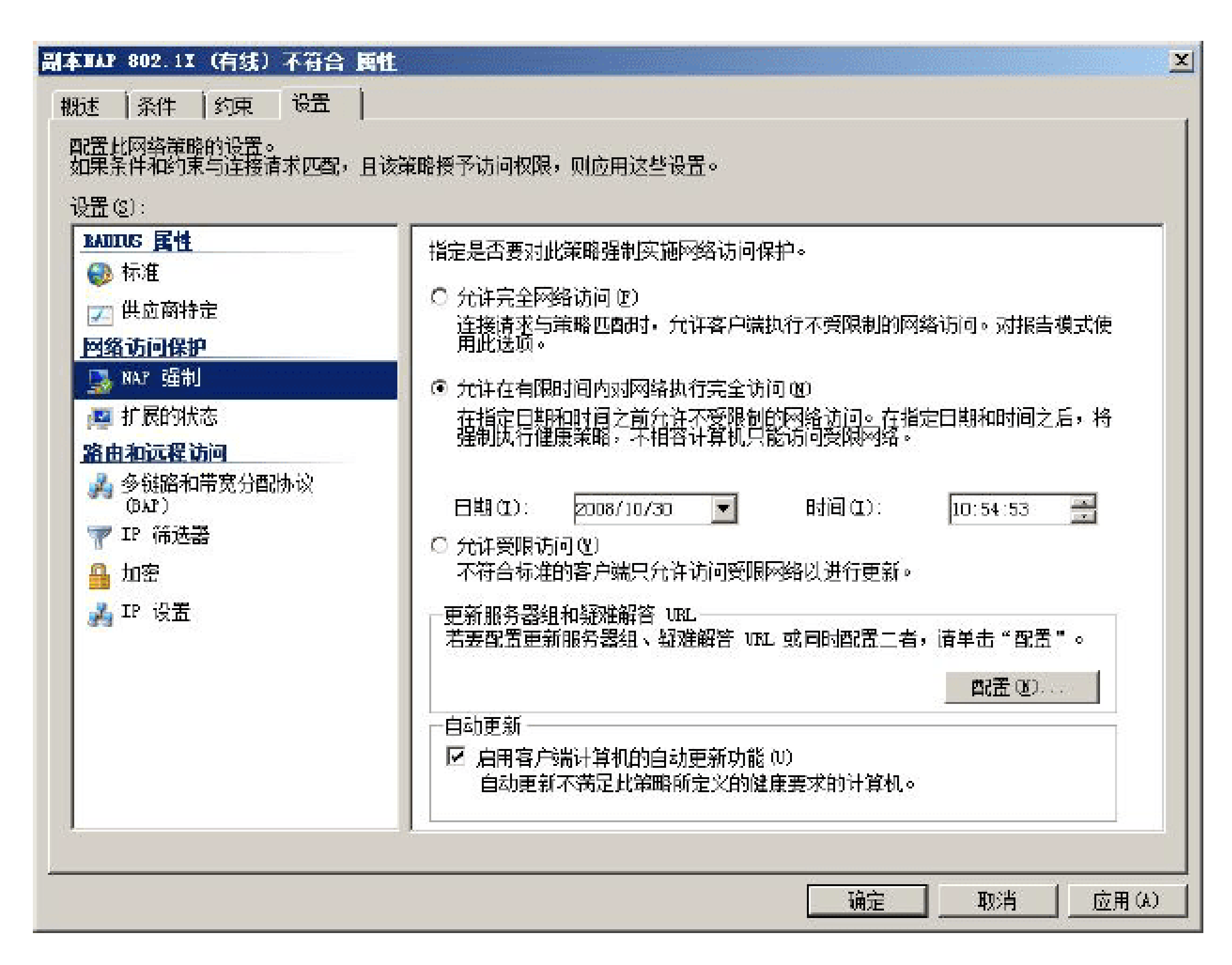


图 14-83 “设置”选项卡

14.2.7 为强制模式配置网络策略

因为已经为不符合的 NAP 客户端的受限访问配置和测试了网络策略，为了启用强制模式，可以修改网络策略副本，并且禁用不符合的 NAP 客户端的初始网络策略。

1. 配置强制模式

① 打开“网络策略服务器”窗口，依次展开“策略”→“网络策略”节点。双击不符合的 NAP 客户端的网络策略副本，打开“策略副本 属性”对话框。

② 切换到“条件”选项卡，在“条件”列表中，选择“Windows 组”选项，单击“删除”按钮，如图 14-84 所示。

③ 切换到“设置”选项卡，在“网络访问保护”区域，单击“NAP 强制”选项。在“自动更新”选项区域，选中“启用客户端计算机的自动更新功能”复选框，如图 14-85 所示。

④ 单击“确定”按钮，保存设置。

⑤ 右击“配置 NAP 向导”创建的不符合的 NAP 客户端的原始网络策略，在弹出的快捷菜单中选择“删除”命令。

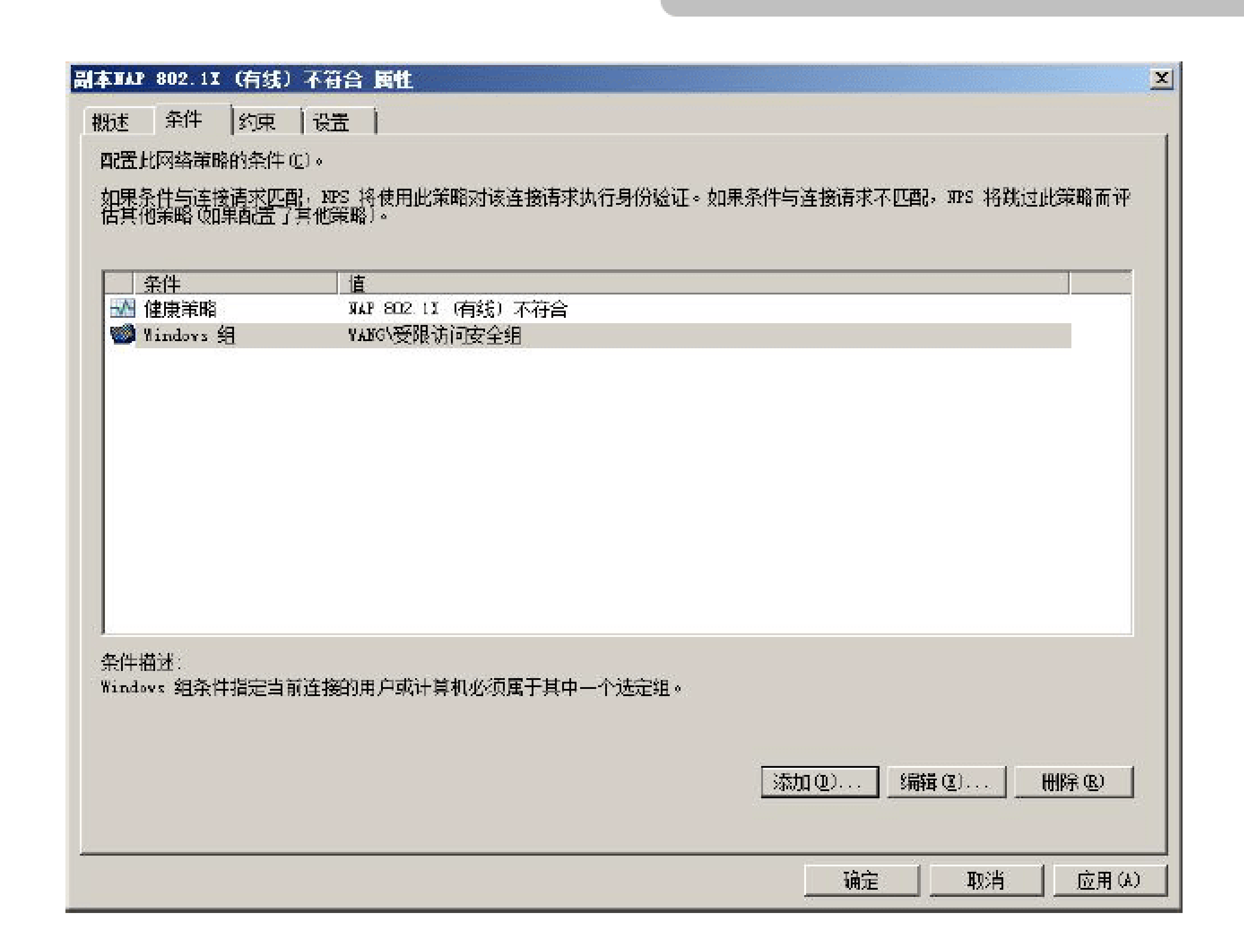


图 14-84　“条件”选项卡

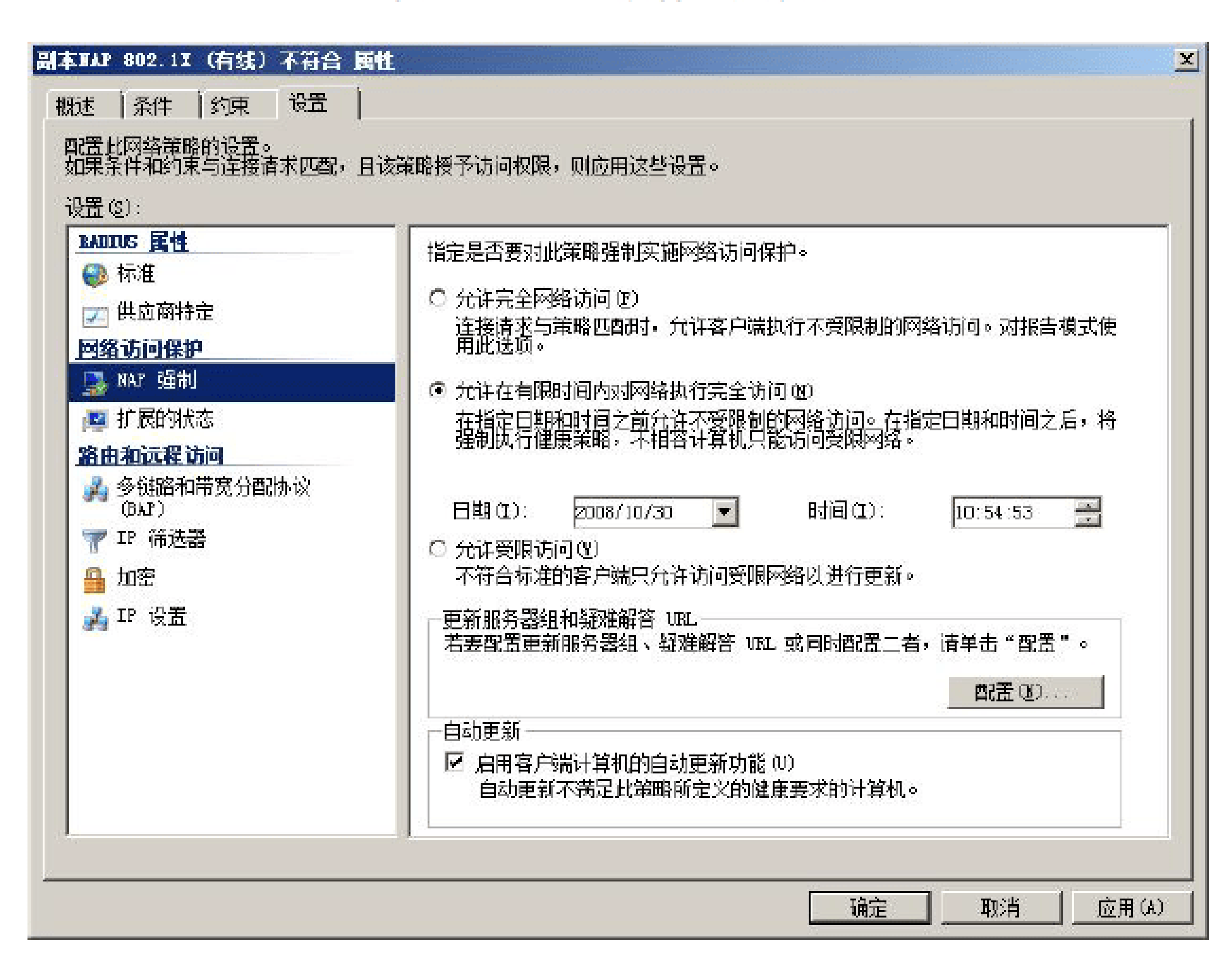


图 14-85　“设置”选项卡

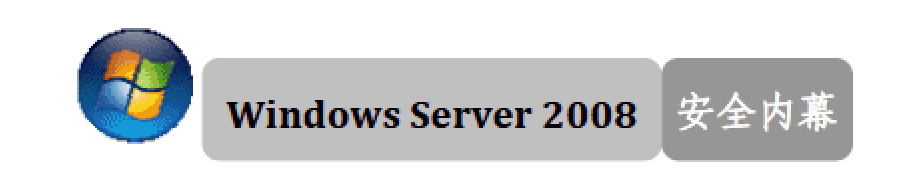
此时，用于测试不符合的 NAP 客户端受限访问的网络策略，将应用于所有 NAP 客户端上，并且删除了原始的不符合的 NAP 客户端的网络策略。

为了限制不支持 NAP 的客户端的访问，在强制模式下，必须为不支持 NAP 的客户端的受限访问配置网络策略。因为不符合的 NAP 客户端的网络策略副本已经配置好，并且经过了测试，可以为不支持 NAP 的客户端复制然后修改该策略。

2. 限制不支持 NAP 的客户端的访问

① 打开“网络策略服务器”窗口，依次展开“策略”→“网络策略”节点。右击不符合的 NAP 客户端的网络策略副本，在弹出的快捷菜单中选择“重复策略”选项，显示如图 14-86 所示的“副本 NAP 802.1X(有线)不符合”窗格。

② 双击新的网络策略，显示如图 14-87 所示的“副本副本 NAP802.1X(有线)不符合 属性”对话框。



在“策略名称”文本框中，输入新的网络策略的名称。在“策略状态”区域，选中“策略已启用”复选框。

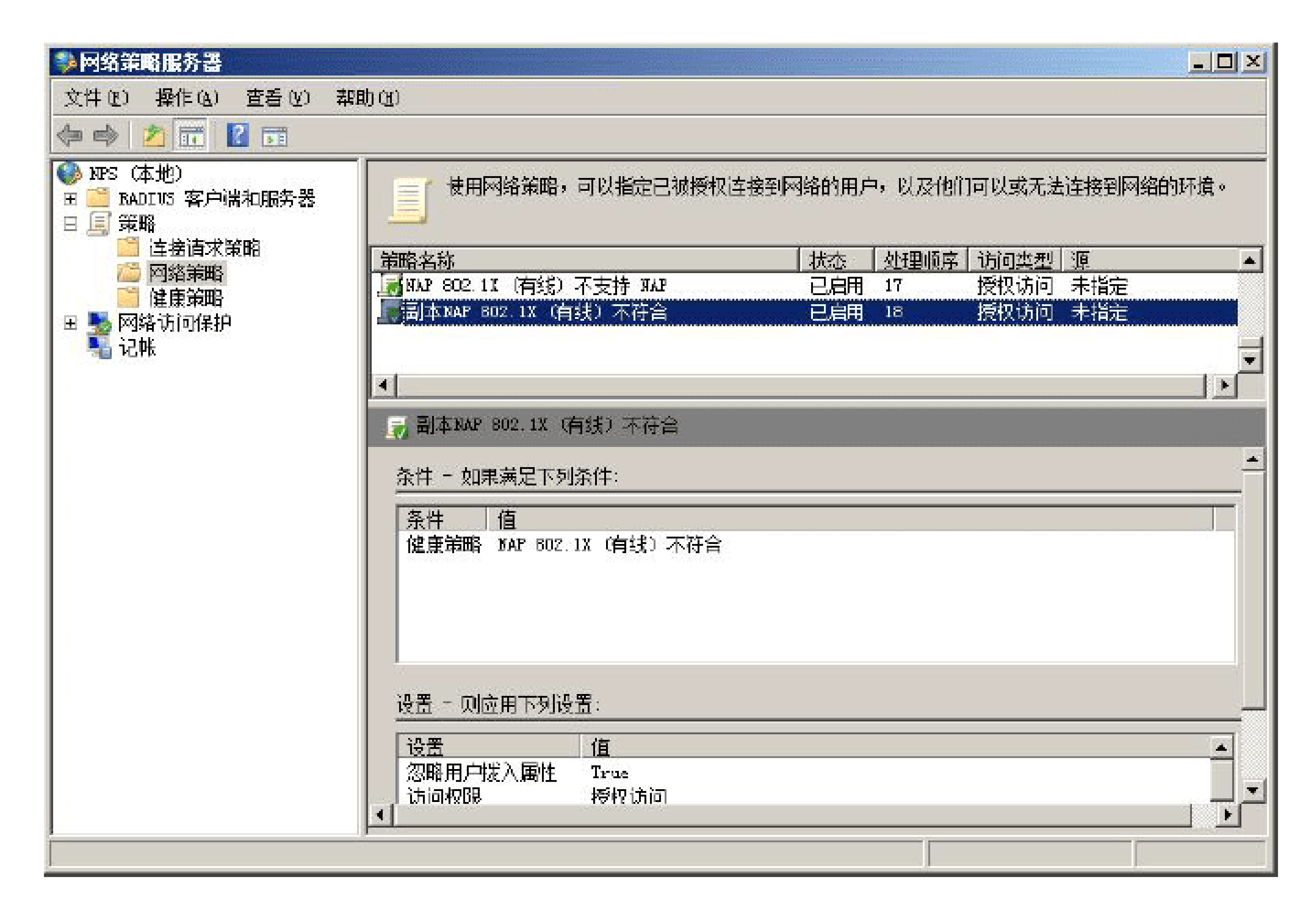
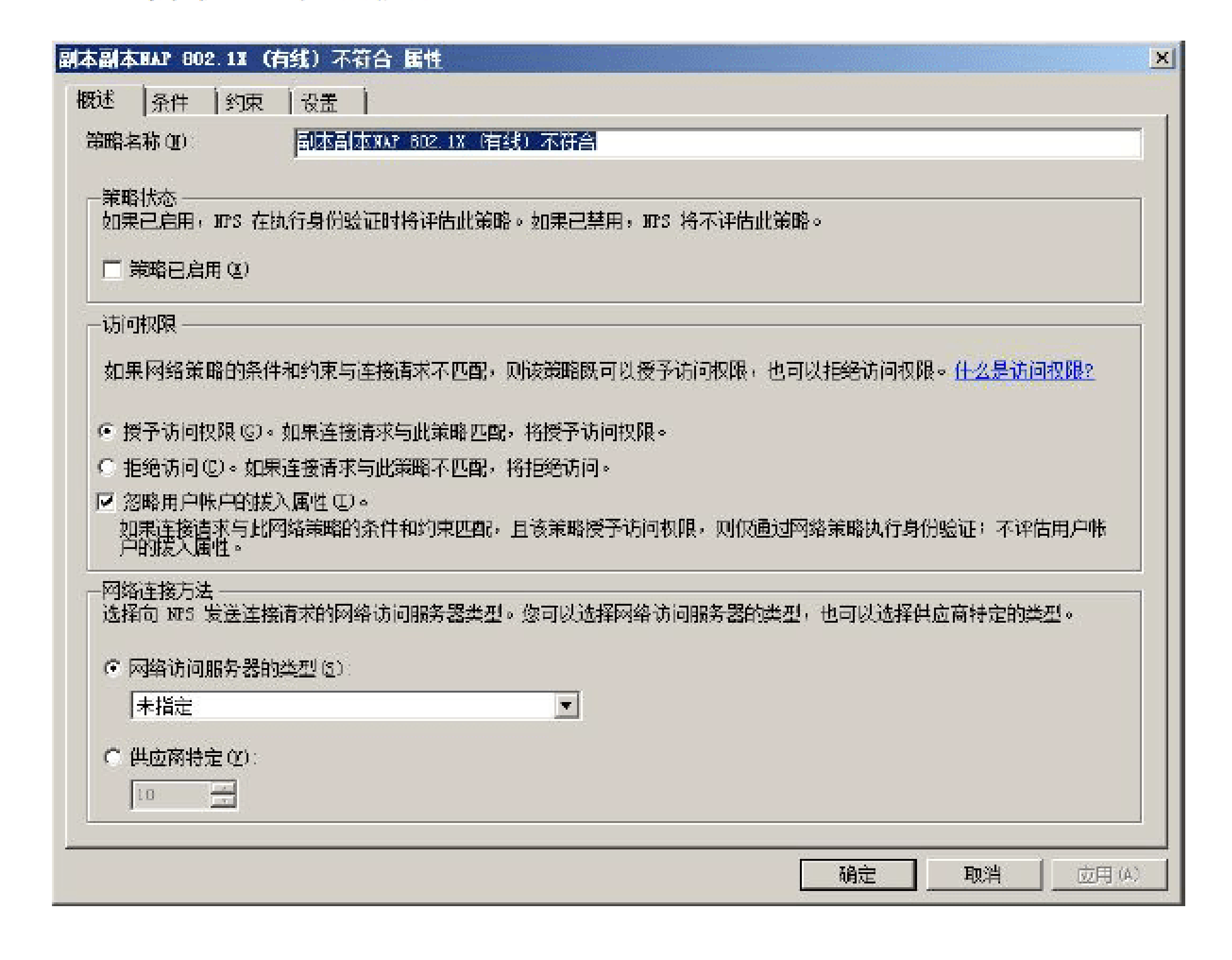


图 14-86 “副本 NAP 802.1X(有线)不符合”窗格

③ 切换到“条件”选项卡，单击“添加”按钮，打开“选择条件”对话框。双击“支持 NAP 的计算机”选项，显示如图 14-88 所示的“支持 NAP 的计算机”对话框，选择“仅限不支持 NAP 的计算机”单选按钮。



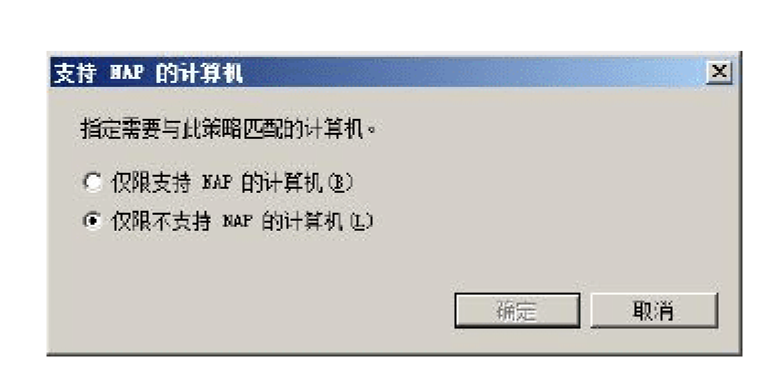


图 14-87 “副本副本 NAP 802.1X(有线)不符合 属性”对话框　　图 14-88 “支持 NAP 的计算机”对话框

④ 单击“确定”按钮，返回到“条件”选项卡。选择“健康策略”选项，单击“删除”按钮，将其删除。最终确认仅保留“支持 NAP”条件即可。

⑤ 单击“确定”按钮，保存设置。在“网络策略服务器”窗口中，移动新建的网络策略直至其位于原始网络策略之上。

⑥ 右击“配置 NAP 向导”创建的不符合的 NAP 客户端的原始网络策略，在弹出的快捷菜单中选择“删除”命令，删除原策略。

至此，802.1X 强制的配置完成。不符合的 NAP 客户端和不支持 NAP 的客户端，即可通过 ACL 或 VLAN 来限制访问。

14.3　配置 VPN 强制

对 VPN 强制的工作过程有所了解之后，即可开始在网络中部署 VPN 强制。需要注意的是，某些环节对系统或网络策略安全性配置要求比较高，如果服务器分配不够合理，则可能导致应用故障。如果条件允许，建议为每个服务器角色选择单独的服务器，以免由于彼此之间的系统环境需求不同，而导致兼容问题。

14.3.1　为 VPN 服务器配置 EAP 身份验证

如果用户没有为远程访问 VPN 连接使用基于 EAP 的身份验证方法，则必须配置基于 Windows Server 2008 的 VPN 服务器使之运行基于 EAP 的身份验证。

① 在“路由和远程访问”窗口，右击路由和远程访问服务器的名称，在弹出的快捷菜单中选择“属性”命令，显示如图 14-89 所示的服务器属性对话框。

② 切换至如图 14-90 所示的“安全”选项卡。提示，由于安装了 NPS 服务器，必须使用它进行身份验证和记账。



图 14-89　服务器属性对话框



图 14-90　“安全”选项卡

③ 单击“身份验证方法”按钮，显示如图 14-91 所示的“身份验证方法”对话框，选中“可扩展的身份验证协议(EAP)”复选框。

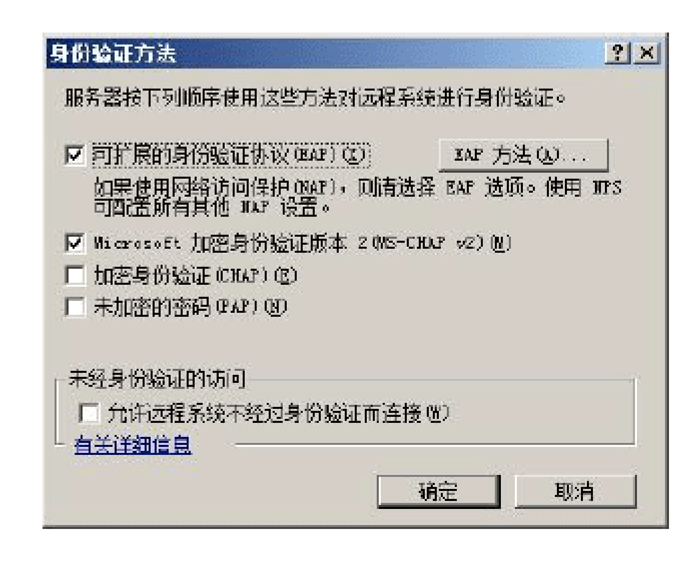


图 14-91　“身份验证方法”对话框

④ 连续两次单击“确定”按钮，保存配置即可。

14.3.2 配置 NAP 健康策略服务器

VPN 强制的 NAP 健康策略服务器，与远程访问 VPN 身份验证所使用的 NPS RADIUS 服务器相同。为了配置 NAP 健康策略服务器，用户必须对现有 NPS 服务器进行如下配置。

- 申请计算机验证证书
- 安装和配置 SHV
- 配置 RADIUS 服务器设置
- 配置 VPN 强制的健康要求策略

1. 申请计算机验证证书

① 在 NPS 服务器上，单击“开始”→“运行”命令，在打开的“运行”对话框的“打开”文本框中输入“mmc”并按 Enter 键，打开“控制台”窗口。

② 单击“文件”→“添加或删除管理单元”命令，显示如图 14-92 所示的“添加或删除管理单元”对话框，在“可用的管理单元”列表框中，选择“证书”单元。

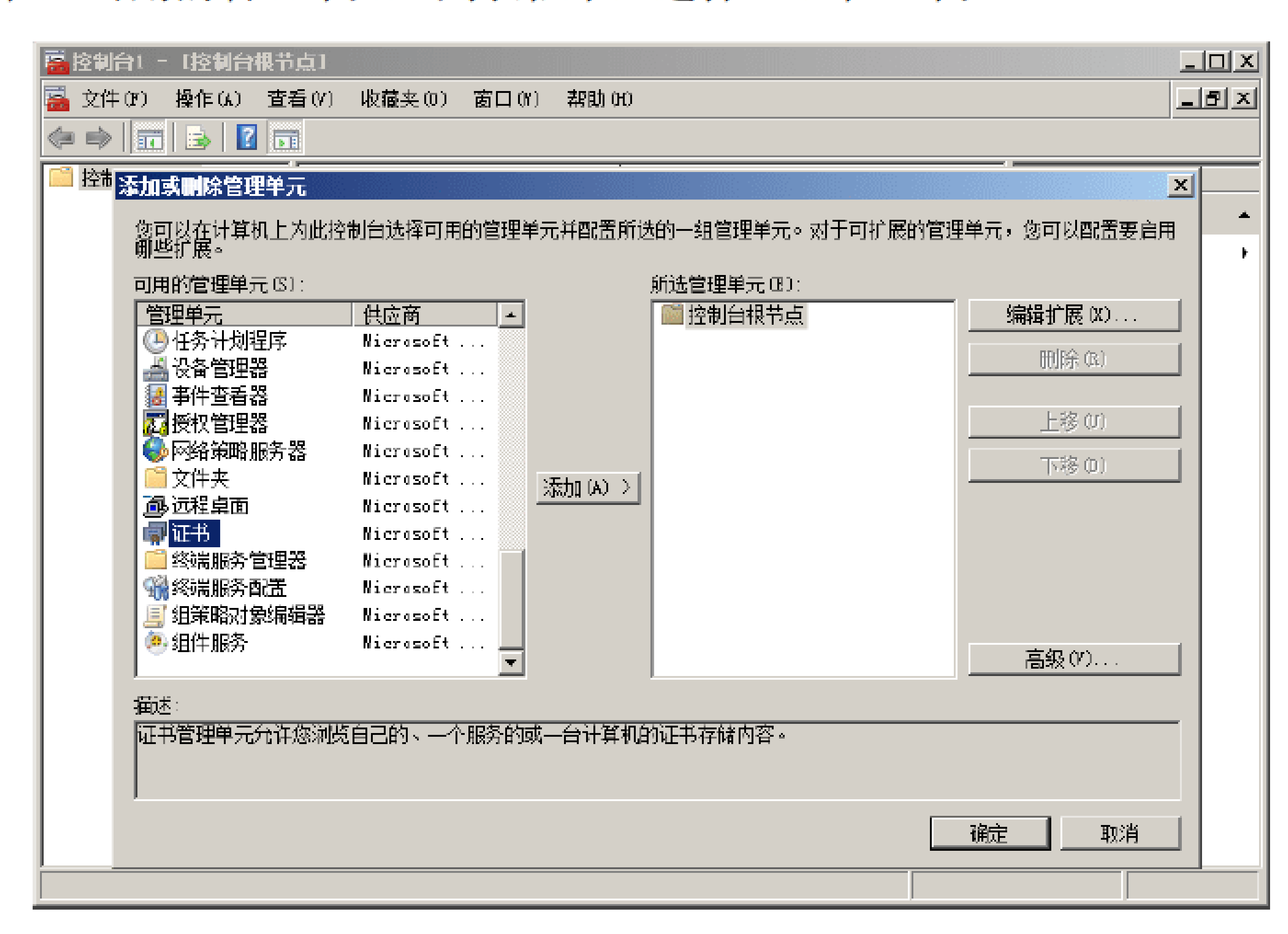


图 14-92 “添加或删除管理单元”对话框

③ 单击“添加”按钮，显示如图 14-93 所示的“证书管理单元”对话框，选择“计算机账户”单选按钮。

④ 单击“下一步”按钮，在“选择计算机”对话框中，选择“本地计算机”单选按钮。

⑤ 依次单击“完成”和“确定”按钮，返回“控制台”窗口。

⑥ 在“控制台”窗口中，依次展开“证书(本地计算机)”→“个人”，右击“个人”并依次选择“所有任务”→“申请新证书”命令，显示如图 14-94 所示的“在您开始前”界面。

⑦ 单击“下一步”按钮，显示如图 14-95 所示的“申请证书”界面，选中“计算机”复选框。

⑧ 单击“注册”按钮，开始向网络中的 CA 提交证书申请，稍等即可成功。单击“完成”按钮，返回“控制台”窗口，如图 14-96 所示。

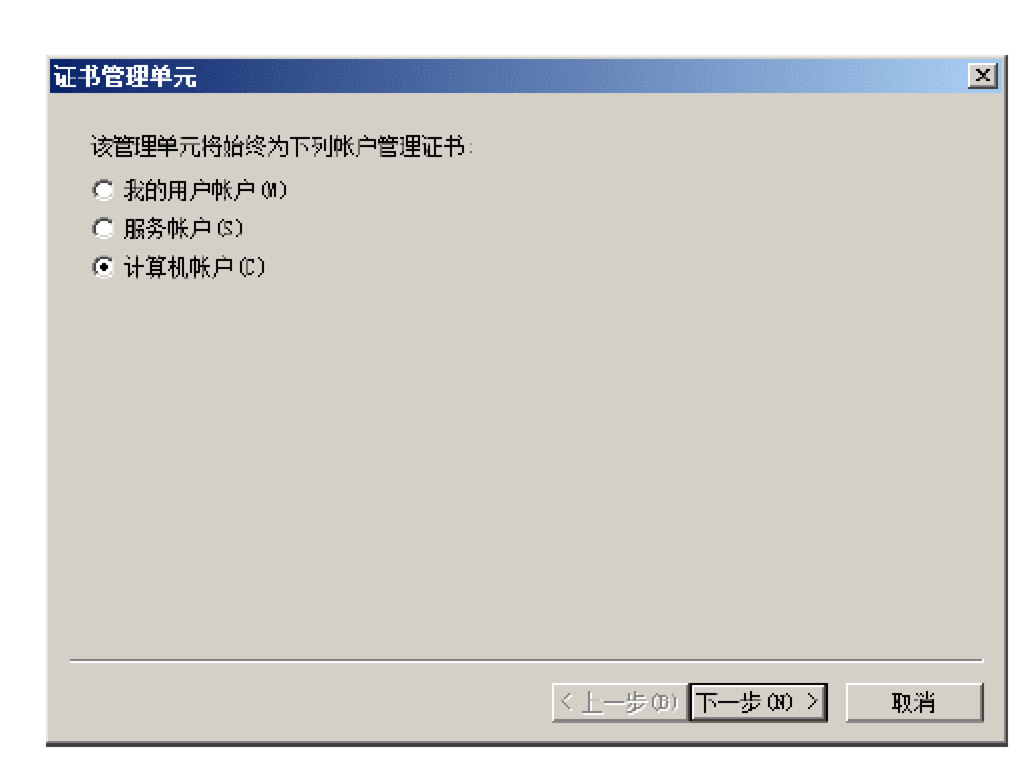


图 14-93　“证书管理单元”对话框



图 14-94　“在您开始前”界面

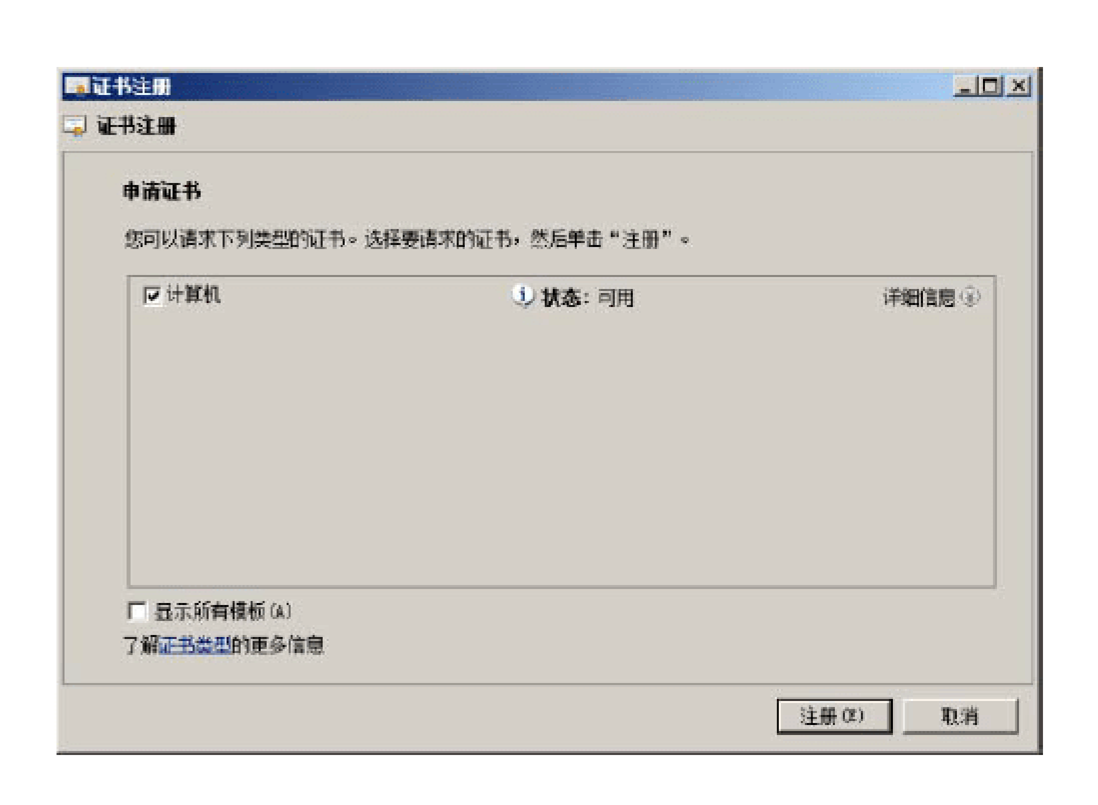



图 14-95　“申请证书”界面

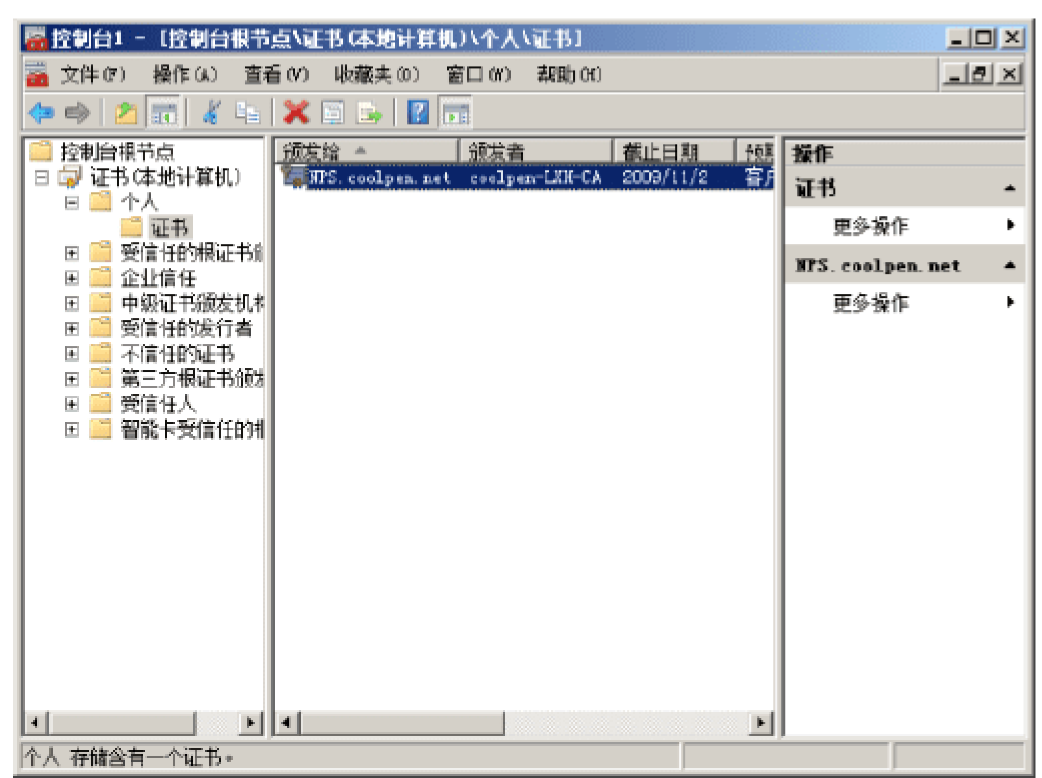


图 14-96　“控制台”窗口

2. 创建 VPN 强制策略

① 在 NPS 服务器上，打开“网络策略管理器”窗口。单击 NPS 选项，在“标准配置”下拉列表框中选择“网络访问保护(NAP)”选项。单击“配置 NAP”超级链接，显示如图 14-97 所示的“选择与 NAP 一起使用的网络连接方法”界面。在“网络连接方法”下拉列表中，选择“虚拟专用网络(VPN)”；在“策略名称”文本框中，输入对应的名称，建议使用默认名称。

② 单击“下一步”按钮，显示如图 14-98 所示的“指定 NAP 强制服务器运行 VPN 服务器”界面。由于 NAP 健康策略服务器已经是一个 RADIUS 服务器，本例中配置 VPN 服务器时，已经将 RADIUS 服务器指向该服务器。需要注意的是，必须在该服务器上设置与之对应的 RADIUS 客户端，双方才可以建立连接。


提示：如果在此之前，管理员在 NPS→“RADIUS 服务器和客户端”中设置了指向 VPN 服务器的 RADIUS 客户端，则将显示在“RADIUS 客户端”列表中。

③ 单击“添加”按钮，显示如图 14-99 所示的“新建 RADIUS 客户端”对话框，在“友好名称”文

本框中，设置适当的名称；在“地址(IP 或 DNS)”文本框中，输入 VPN 服务器的 IP 地址。“共享机密”的方式必须与 VPN 服务器匹配。



图 14-97 “选择与 NAP 一起使用的网络连接方法”界面

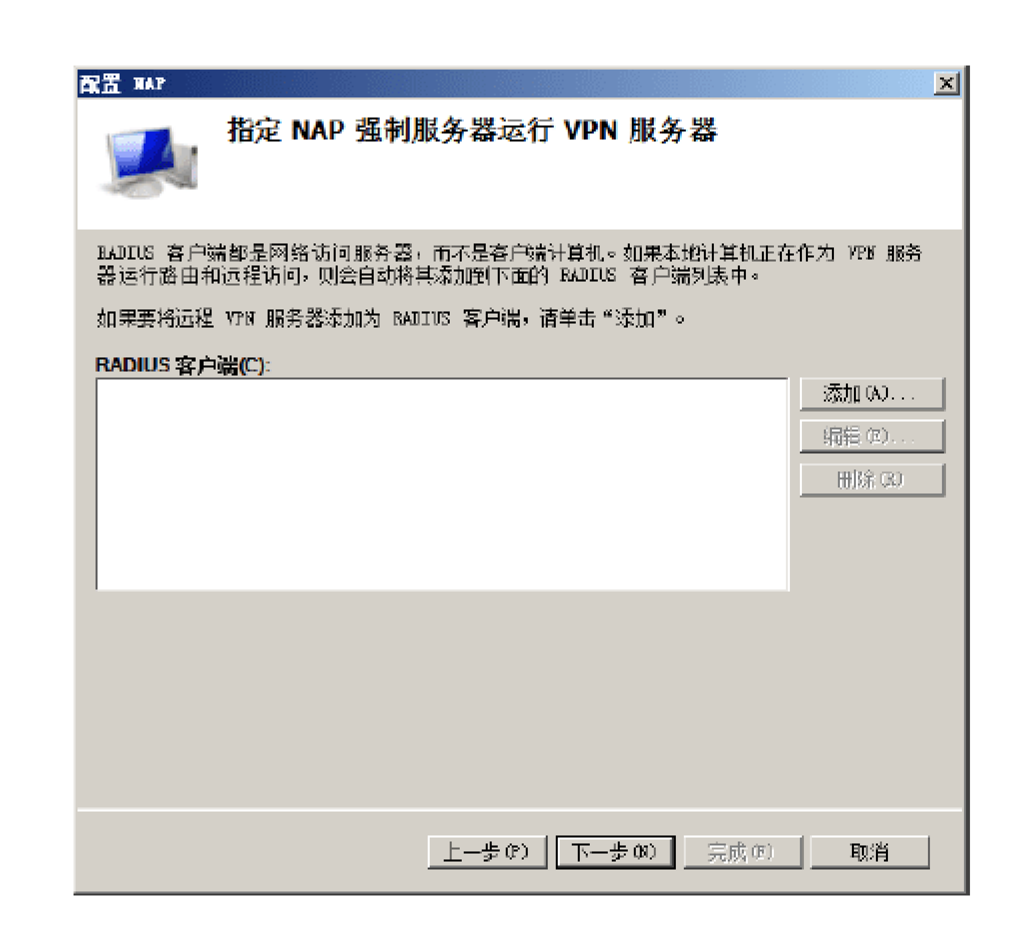


图 14-98 “指定 NAP 强制服务器运行 VPN 服务器”界面

④ 单击“确定”按钮，返回“指定 NAP 强制服务器运行 VPN 服务器”对话框。单击“下一步”按钮，显示如图 14-100 所示的“配置用户组和计算机组”界面，根据需要配置组。如果不选择，则将对所有计算机组和用户组有效。



图 14-99 “新建 RADIUS 客户端”对话框

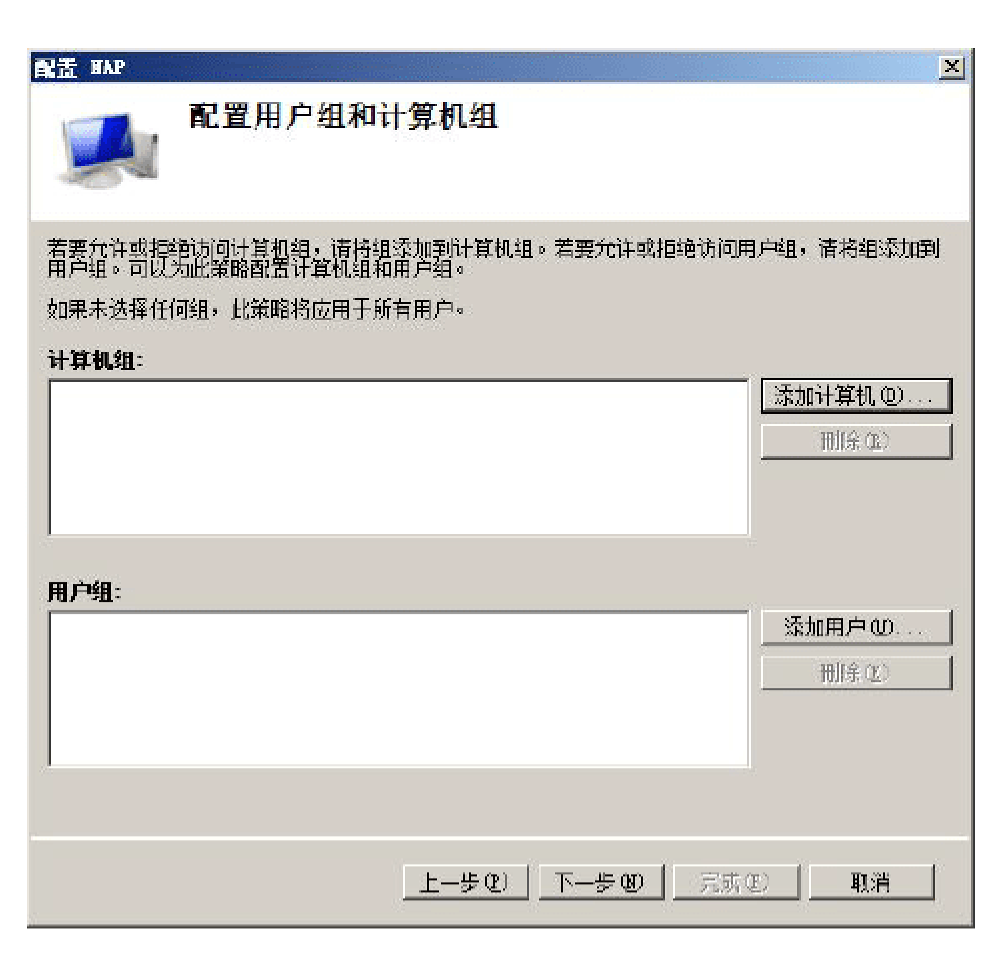


图 14-100 “配置用户组和计算机组”界面

⑤ 单击“下一步”按钮，显示如图 14-101 所示的“配置身份验证方法”界面，为 PEAP 身份验证选择 NPS 所使用的计算机证书，即上述操作中申请的验证证书。根据需要选中“安全密码(PEAP-MS-CHAP v2)”或者“智能卡或其他证书(EAP-TLS)”复选框，需要注意的是，VPN 服务器、NPS 和客户端必须设置完全相同的身份验证方式，否则无法建立连接。如果默认没有使用该证书，则可以单击“选择”按钮，显示“选择证书”对话框，确认为所需证书后单击“确定”按钮即可。

⑥ 单击“下一步”按钮，显示如图 14-102 所示的“指定 NAP 更新服务器组和 URL”界面。更新服务器组的主要作用就是对未通过健康策略审查的被隔离客户端进行“补救”，通常包括 WSUS 服

务器、网络防病毒服务器等。除此之外，也可以根据健康策略的审查重点不同，而不设置更新服务器组，例如仅检测网络防火墙状态。在这里单击“新建组”按钮，可以配置更新服务器组。

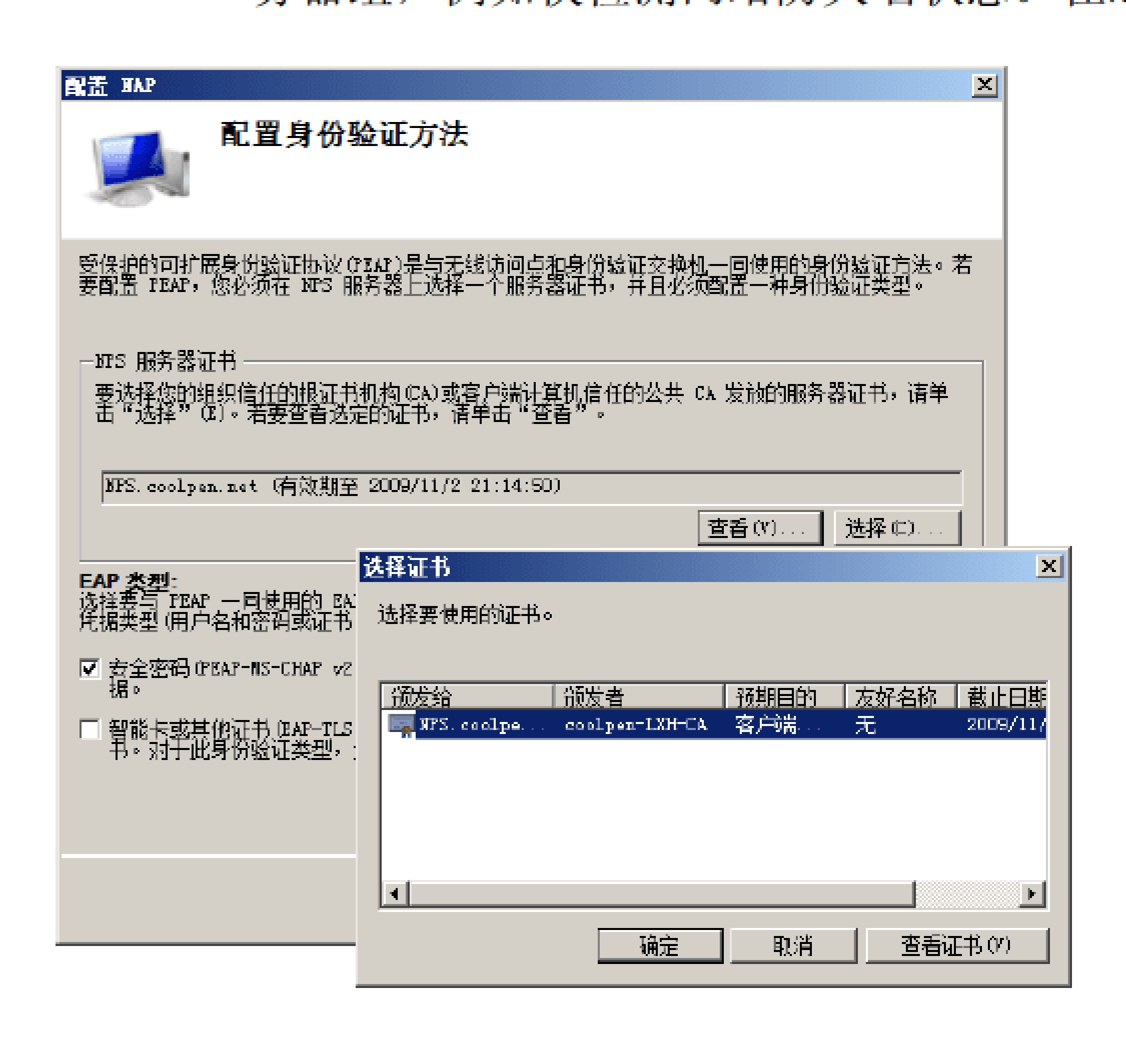


图 14-101　“配置身份验证方法”界面

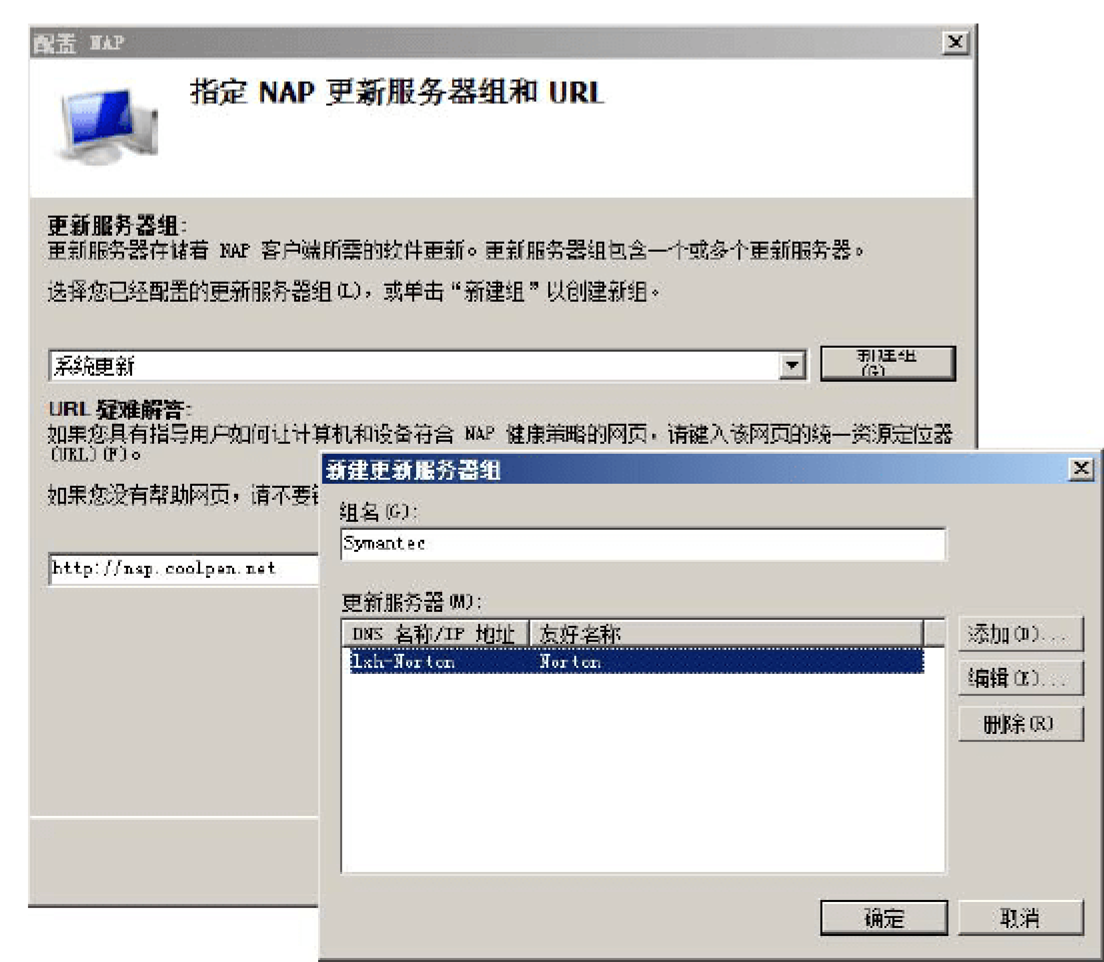


图 14-102　“指定 NAP 更新服务器组和 URL”界面

⑦ 单击“下一步”按钮，显示如图 14-103 所示的“定义 NAP 健康策略”界面，选择 VPN 强制需要评估的 SHV，根据需要选中“启用客户端计算机的自动更新”复选框。选择“允许对不具有 NAP 功能的客户端计算机的完全网络访问权限”单选按钮，即可使用户想要不支持 NAP 功能的客户端拥有受限访问。选中“启用客户端计算机的自动更新”复选框，则当由于客户端计算机的自动更新未开启而未通过策略审核被隔离时，将自动启动客户端的自动更新设置。

⑧ 单击“下一步”按钮，显示如图 14-104 所示的“正在完成 NAP 增强策略和 RADIUS 客户端配置”界面。

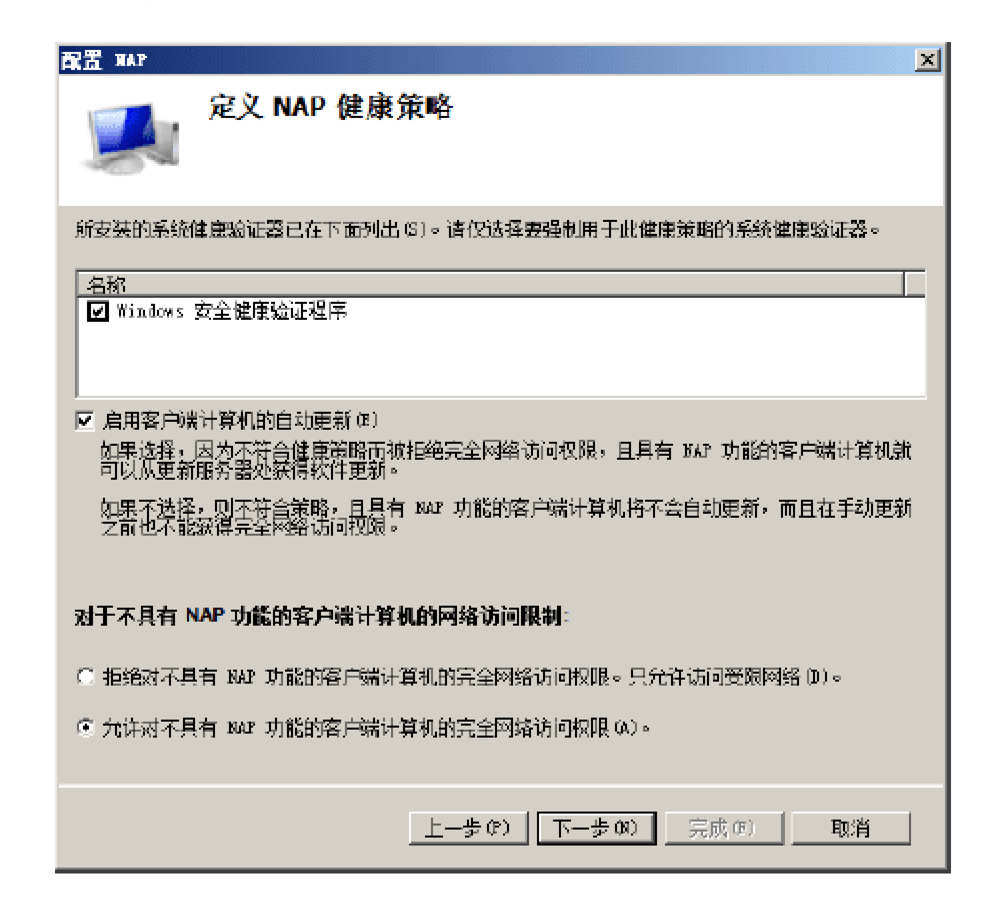


图 14-103　“定义 NAP 健康策略”界面



图 14-104　“正在完成 NAP 增强策略和 RADIUS 客户端配置”界面

⑨ 单击“完成”按钮，关闭“配置 NAP”向导。

“配置 NAP”向导创建的连接请求策略、健康策略和网络策略位于各自顺序列表的底部，直到用户删除或改变现有远程访问 VPN 网络策略，“配置 NAP”向导创建的网络策略才会用于基于 VPN 的远程访问连接的身份验证或健康评估。



提示：为了确保“配置 NAP”向导产生的策略是正确无误的，应在“策略”中的“连接请求策略”、“健康策略”和“网络策略”中，一一检查每条策略的执行顺序、条件、约束和设置等。

3. 安装和配置 SHV

SHV 必须安装在 NAP 健康策略服务器上，进行健康策略评估。NPS 服务包含 Windows 安全健康验证程序 SHV，来指定运行 Windows Vista 或 Windows XP SP3 的 NAP 客户端的 Windows 安全中心设置，包括防火墙、自动更新、防病毒程序、防间谍软件等审核对象。安装其他 SHV 的方法将取决于 SHV 供应商，可以通过供应商主页下载或者运行供应商提供的 CD-ROM 中的安装程序进行安装。配置方法与其他类型强制相同，详细操作请参考本章“配置 IPSec 强制”中的相关内容。

4. 为 RADIUS 客户端配置 NAP 支持

NAP 健康策略服务器已经为远程访问 VPN 完成连接配置。对于 VPN 连接，用户必须在 VPN 相应的 RADIUS 客户端属性对话框中，选中“RADIUS 客户端支持 NAP”复选框。用户也可以从“网络策略管理器”管理单元的“RADIUS 客户端”节点中更改 RADIUS 客户端的属性。由于 VPN 强制配置将使用报告模式，不符合的 NAP 客户端拥有不受限的访问，所以用户在启用强制模式之前，可能需要更改 NAP 健康策略服务器的登录入站请求。

在“网络策略服务器”管理单元中，依次展开“NPS(本地)”→“RADIUS 客户端和服务器”→“RADIUS 客户端”节点。右击名称为 VPN 的 RADIUS 客户端，选择快捷菜单中的“属性”命令，显示如图 14-105 所示的“vpn 属性”对话框，选中“RADIUS 客户端支持 NAP”复选框。

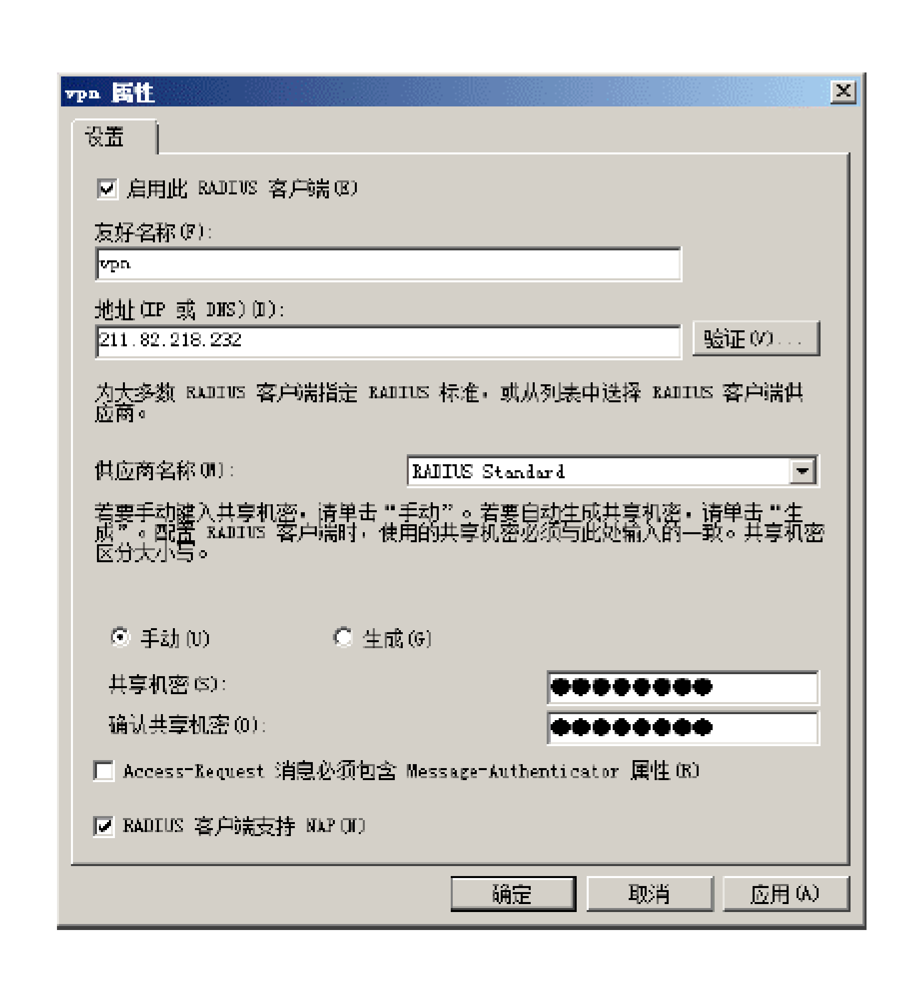


图 14-105 “vpn 属性”对话框

14.3.3 配置 NAP 客户端

由于 VPN 客户端建立到 VPN 服务器的连接之前，需要先通过 NPS 服务器的健康评估，所以与常规 VPN 客户端配置有所不同。配置 NAP 客户端的基本步骤如下。

- 下载客户端计算机证书
- 安装 SHA
- 创建和配置 VPN 客户端
- 通过组策略配置可管理的 NAP 客户端

1. 下载验证证书

客户端计算机必须登录域中的 CA，获取所需的验证证书。

① 打开 IE 浏览器，按照 http://CA 服务器/certsrv 方式登录 CA，显示如图 14-106 所示窗口。

注意：集成在域控制器上的 CA，默认情况下，已禁止“允许匿名访问”方式，此时可以联系域管理员，登录证书服务器，并在 IIS 管理器中，启用 CA 站点以及 Certsrv 目录的“允许匿名访问”身份验证方式。

② 单击“下载 CA 证书、证书链或 CRL”链接，显示如图 14-107 所示的下载 CA 证书、证书链或 CRL 窗口。单击“下载 CA 证书”超级链接，显示“文件下载-安全警告”对话框。

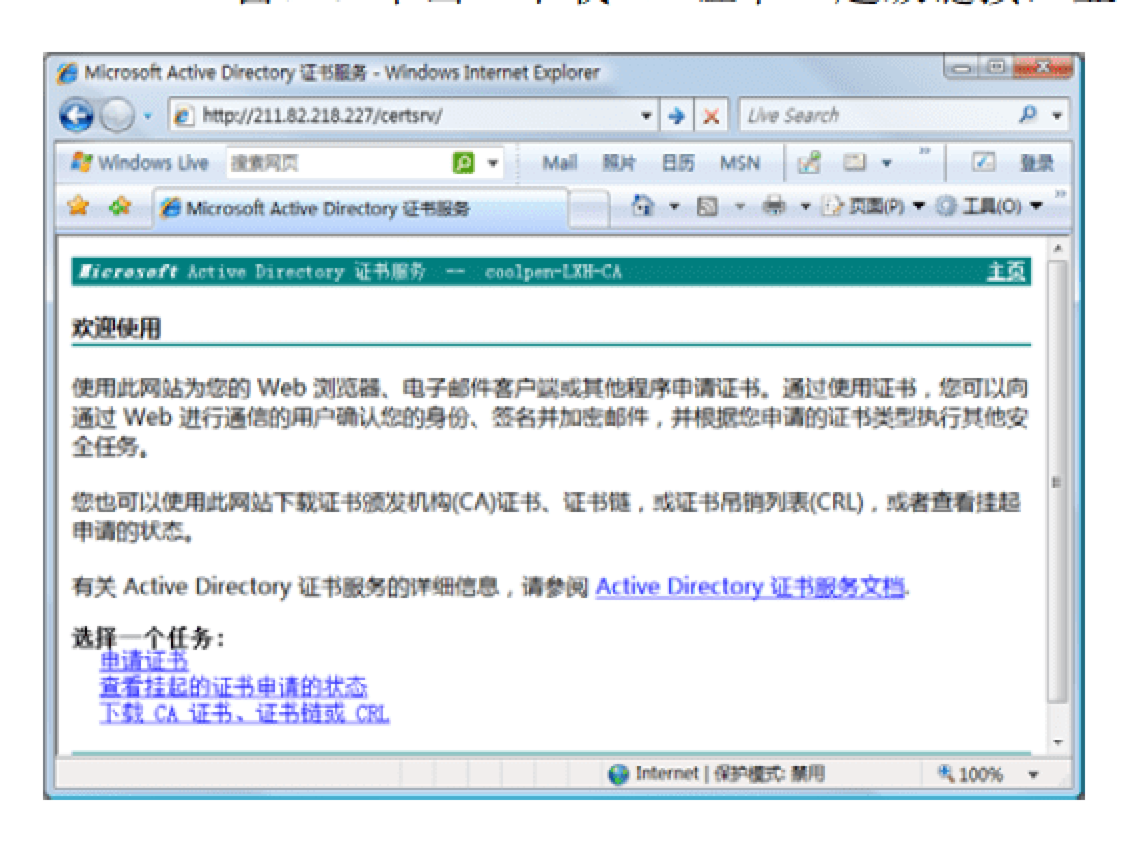


图 14-106　登录证书服务器

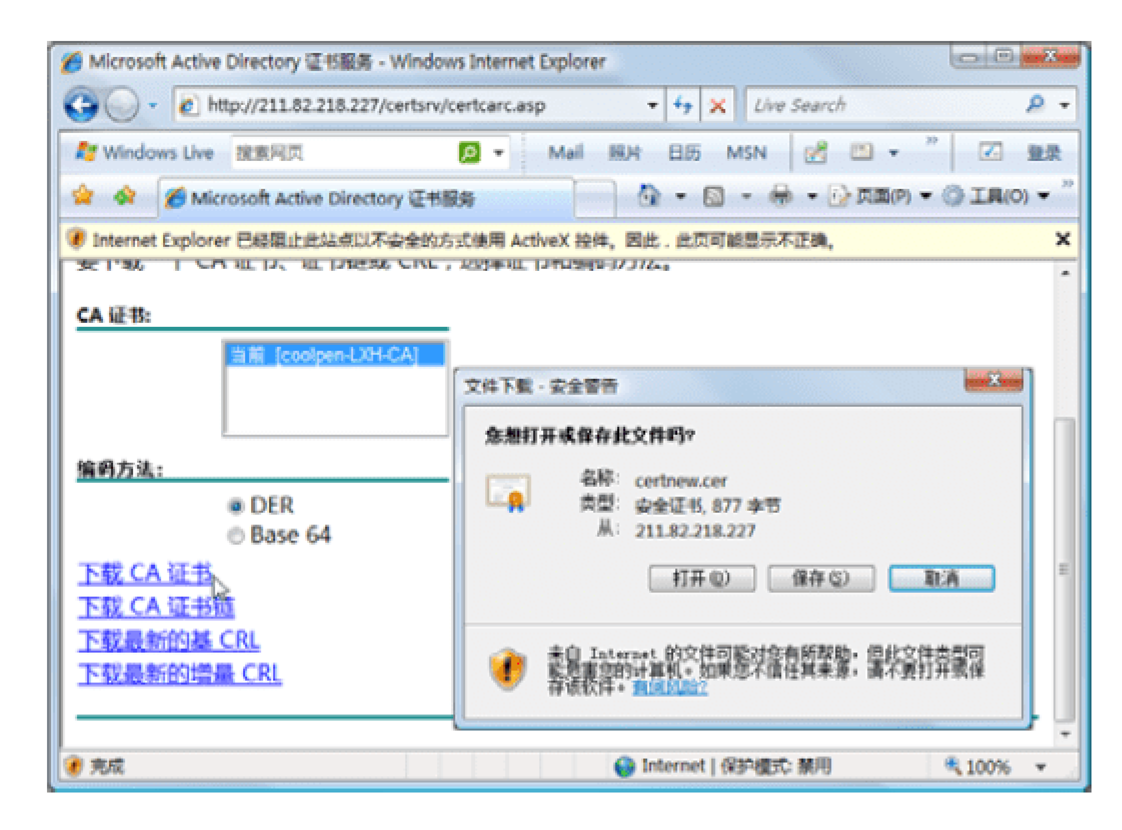


图 14-107　下载 CA 证书、证书链或 CRL 窗口

③ 可以单击“保存”按钮，先将证书保存到本地计算机，然后再安装到相应的目录下；也可以单击“打开”按钮，直接开始安装。

安装过程中需要注意的是，在“证书存储”步骤，需要选择“将所有的证书放入下列存储”单选按钮，并单击“浏览”按钮，打开“选择证书存储”对话框，选择“受信任的根证书颁发机构”目录，如图 10-108 所示。

2. 创建和配置 VPN 客户端

VPN 客户端连接的创建比较简单，详细操作过程可参考本书第 11 章中的相关介绍，此处不复赘述。配置 VPN 强制时，注意客户端身份验证协议是否正确，应确保与 VPN 服务器完全一致，否则将无法建立连接。

① 在“网络连接”窗口中，右击创建的 VPN 连接，选择快捷菜单中的“属性”命令，打开“coolpen 属性”对话框。切换至“安全”选项卡，选择“高级(自定义设置)”单选按钮，如图 14-109 所示。

② 单击“设置”按钮，显示如图 14-110 所示的“高级安全设置”对话框，在“数据加密”下拉列表框中选择“需要加密(如果服务器拒绝将断开连接)”选项，选择“使用可扩展的身份验证协议(EAP)”单选按钮，并选择下拉列表框中的“受保护的 EAP(PEAP)”选项。

③ 单击“属性”按钮，显示如图 14-111 所示的“受保护的 EAP 属性”对话框，取消选中“连接到这些服务器”复选框。选中“验证服务器证书”复选框，在“受信任的根证书颁发机构”列表框中，会发现已经安装的证书颁发机构。在“选择身份验证方法”下拉列表框中，选择“安全密码(EAP-MSCHAP v2)”选项。选中“启用隔离检查”复选框。

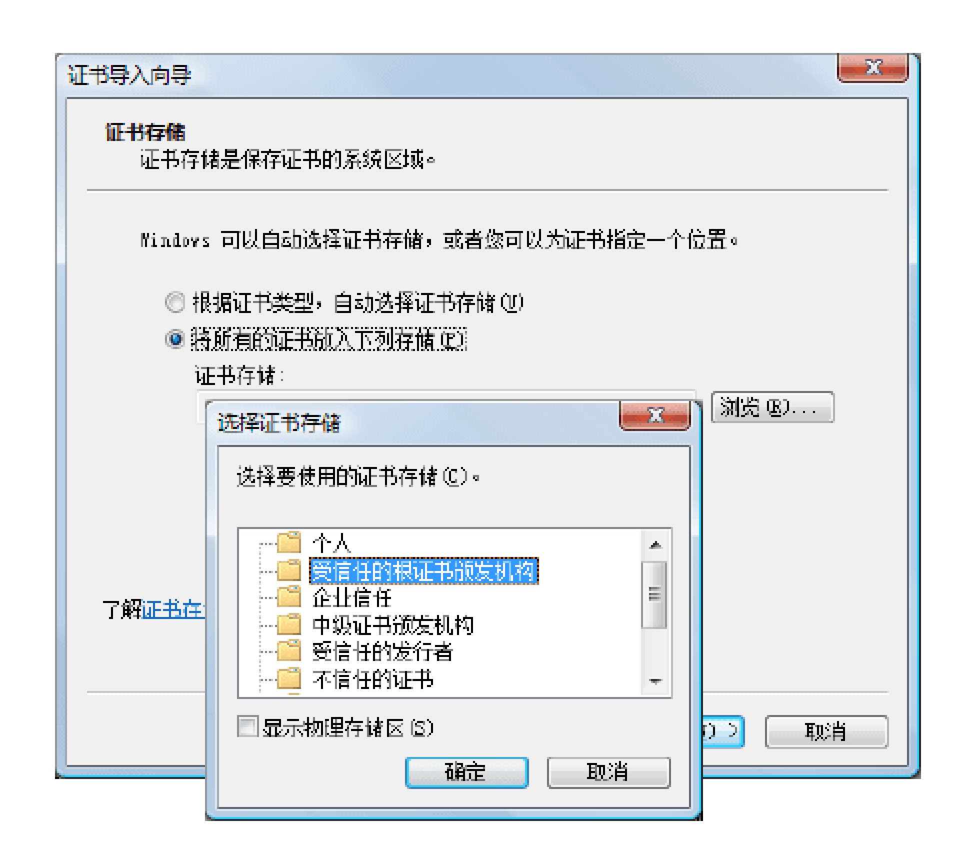


图 14-108 “证书存储”界面

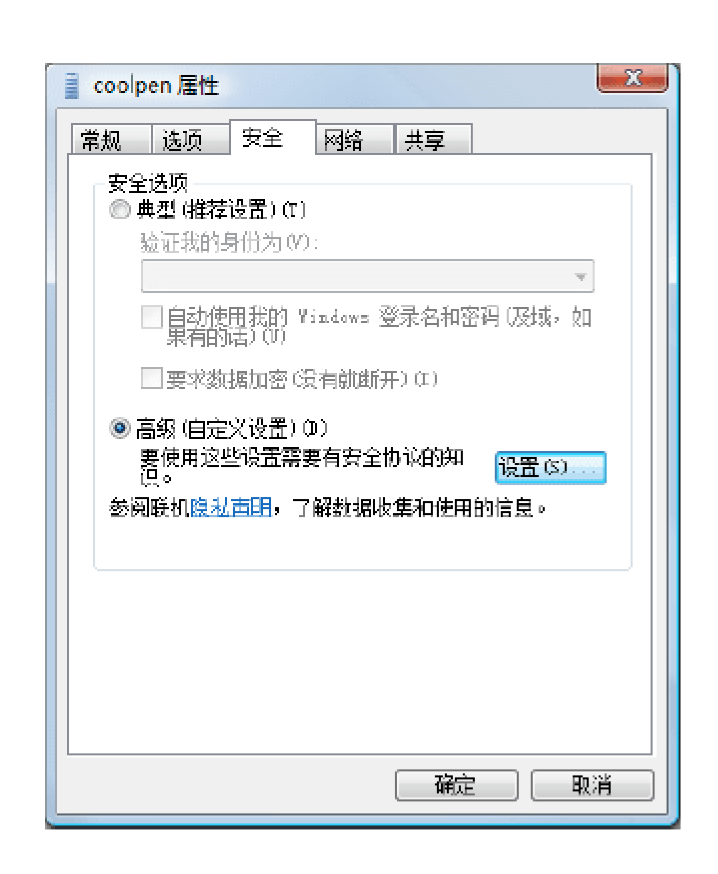


图 14-109 “安全”选项卡

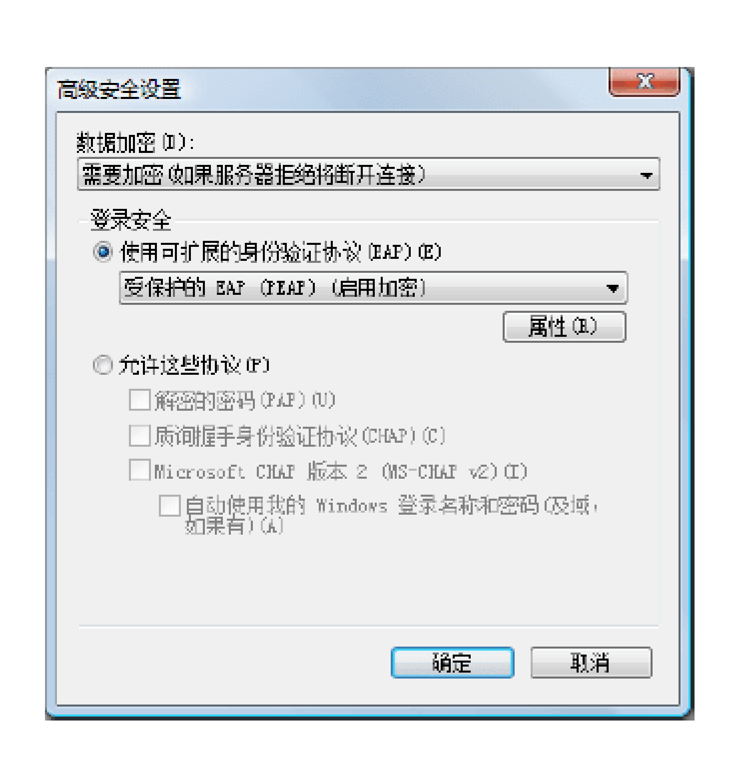


图 14-110 “高级安全设置”对话框

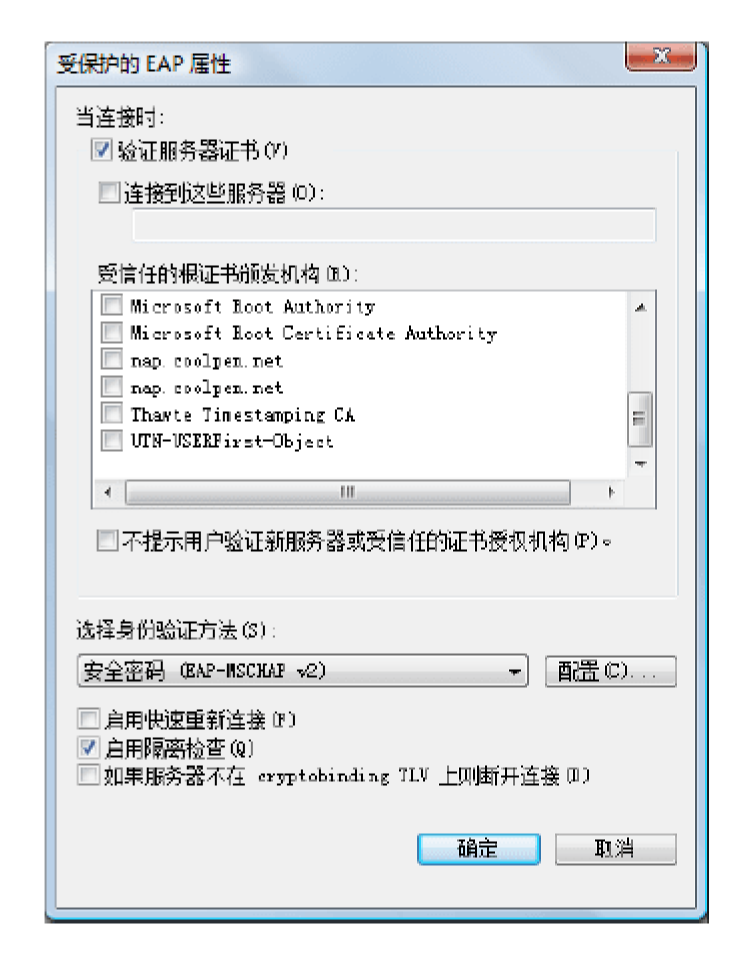


图 14-111 “受保护的 EAP 属性”对话框

3. 通过组策略配置 NAP 客户端

对于可管理的 NAP 客户端，管理员可以使用组策略进行 NAP 客户端的设置，主要包括如下步骤。

- 配置 NAP 客户端设置
- 启用 Windows 安全中心(请参考 IPSec NAP 客户端的配置)
- 配置网络访问保护代理服务的自动启用(请参考 IPSec NAP 客户端的配置)

在“组策略管理器”管理单元中，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“网络访问保护”→“NAP 客户端配置”节点，双击“远程访问隔离强制客户端”，显示如图 14-112 所示的“远

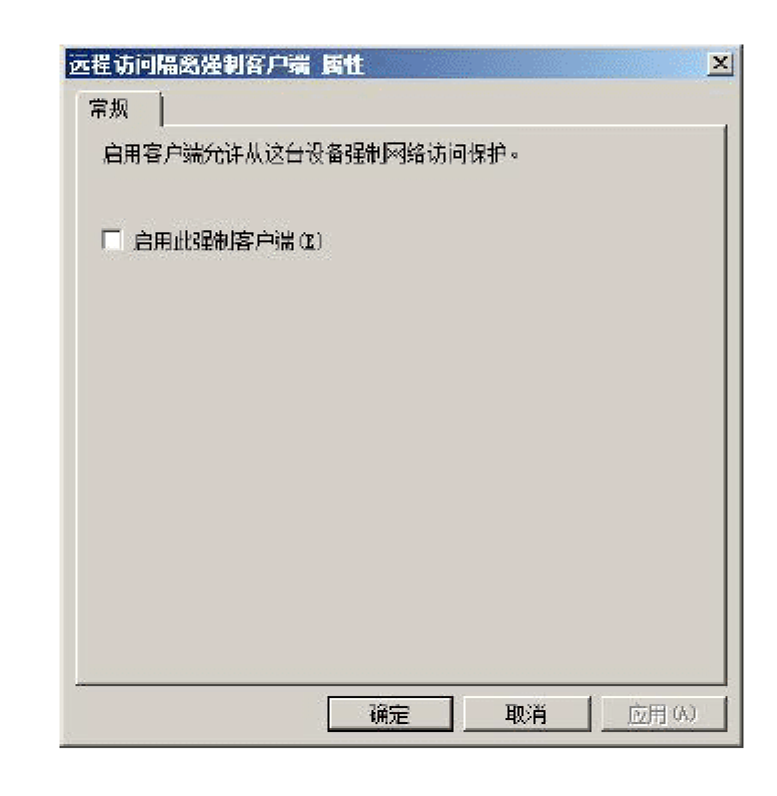


图 14-112 “远程访问隔离强制客户端 属性”对话框

程访问隔离强制客户端 属性”对话框，选中“启用此强制客户端”复选框。单击“确定”按钮，保存设置。

14.3.4　测试受限 VPN 客户端的访问

在启用强制模式之前，用户必须测试不符合的 NAP 客户端的受限访问，以确保其可以被提示未通过评估的原因，并且只能访问受限网络中的补救服务器。

① 在“网络连接”窗口中，双击 VPN 连接，输入用户名和密码并单击“确定”按钮，即可尝试连接到 VPN 服务器。由于已经设置健康策略验证，所以 VPN 客户端必须先提供验证证书，如图 14-113 所示。

② 单击“确定”按钮，尝试连接到 VPN 服务器。此时，由于防火墙设置不符合健康策略要求，任务栏中会显示“此计算机不符合该网络的要求”信息，如图 14-114 所示。

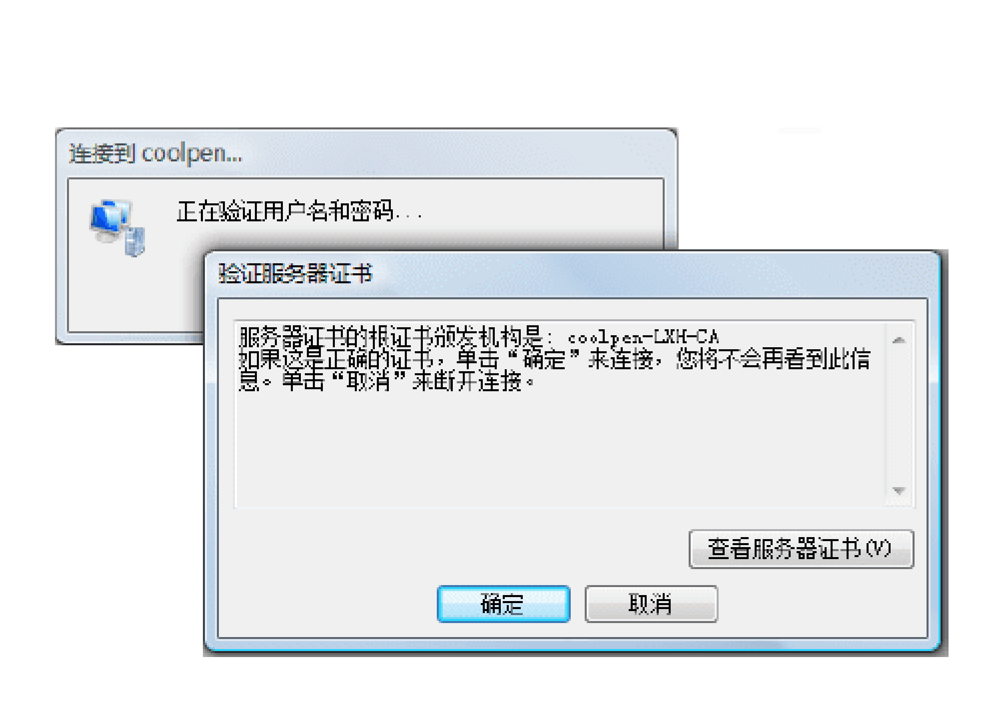


图 14-113　“验证服务器证书”对话框

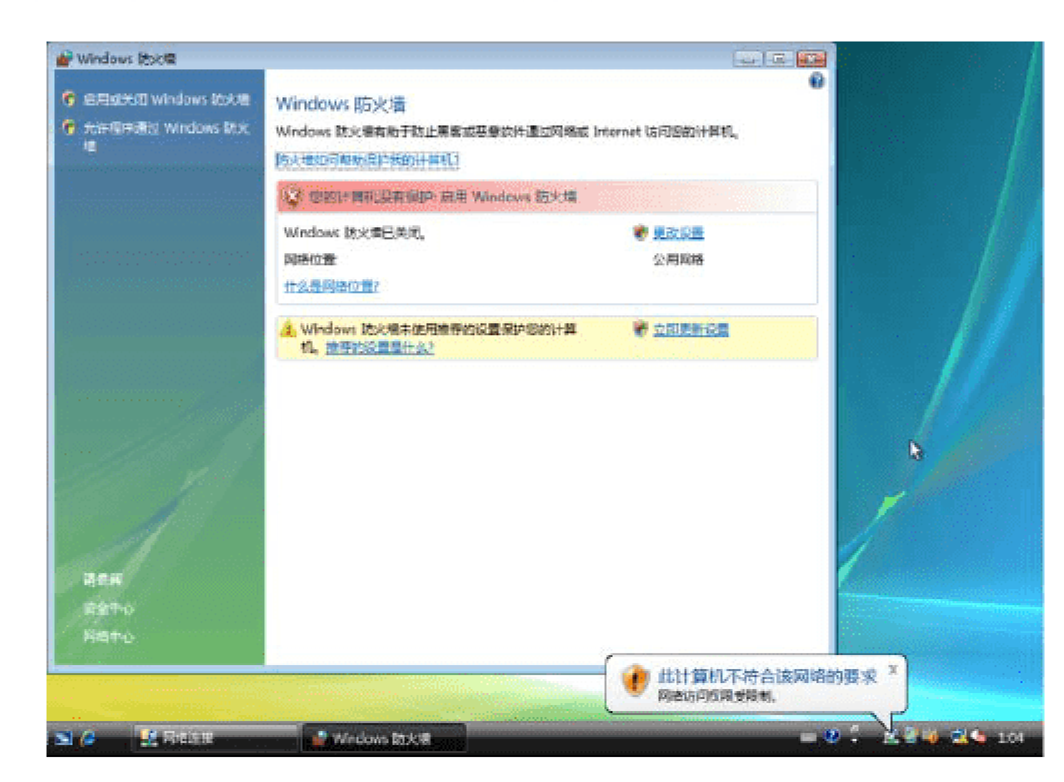
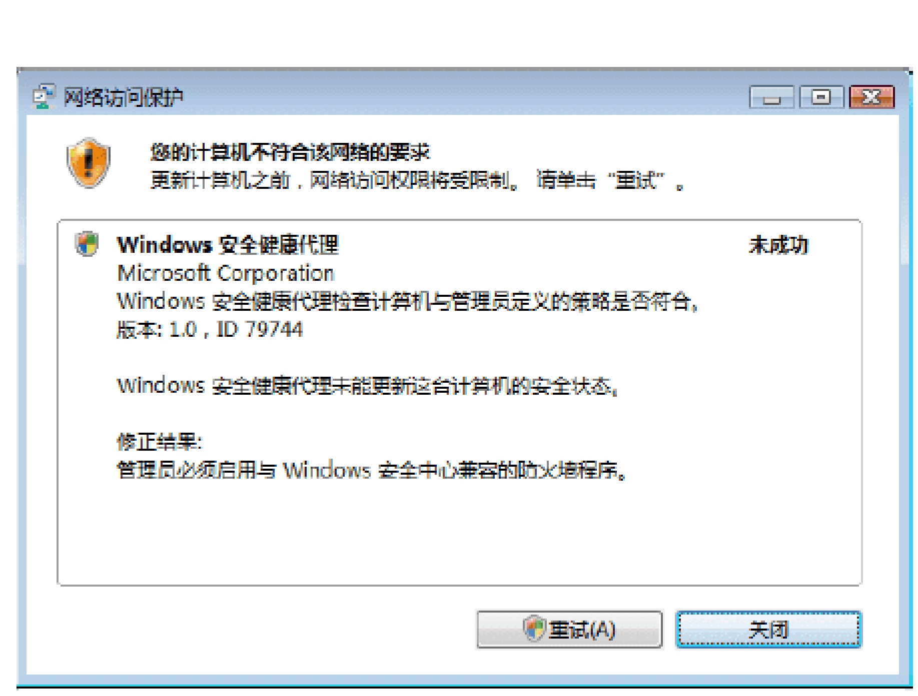


图 14-114　此计算机不符合该网络的要求

③ 单击信息提示框，显示如图 14-115 所示的“网络访问保护”对话框。当前验证结果为“未成功”，修正结果为“管理员必须启用与 Windows 安全中心兼容的防火墙程序”。

④ 根据提示信息，启用 Windows 防火墙后，任务栏中将自动显示如图 14-116 所示的提示信息“此计算机符合该网络的要求”。



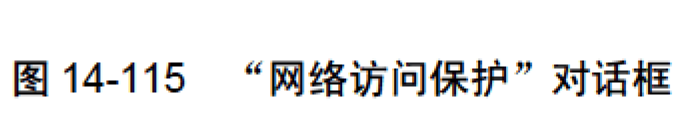

图 14-115　“网络访问保护”对话框



图 14-116　此计算机符合该网络的要求

⑤ 此时单击信息框，显示如图 14-117 所示的“您的计算机符合该网络的要求”界面，即完全符合健

康策略的要求。

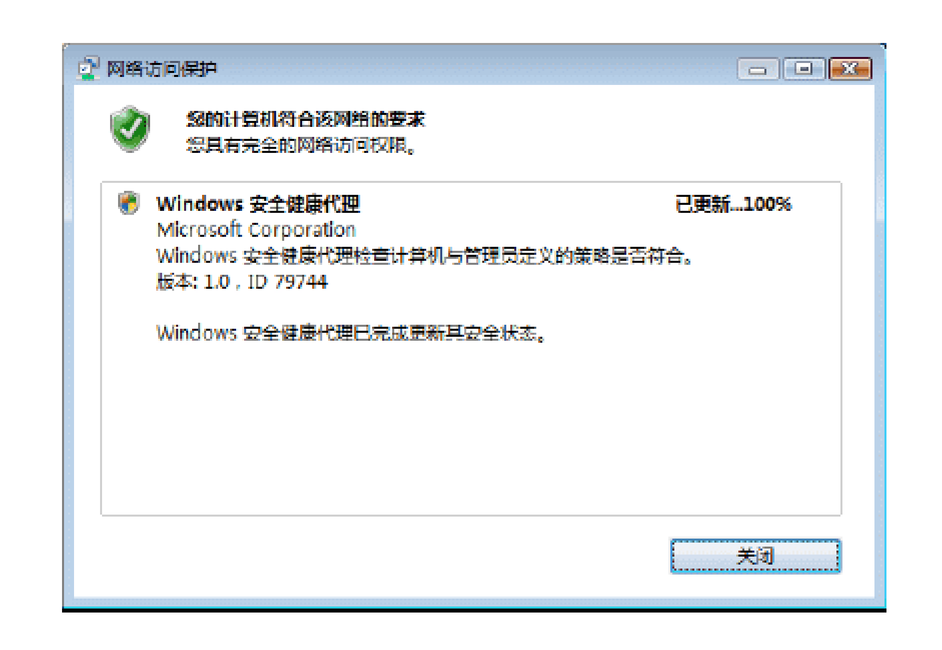


图 14-117 “您的计算机符合该网络的要求”界面

14.3.5 配置强制模式网络策略

管理员为不符合的 NAP 客户端的受限访问配置和测试了网络策略之后，即可启用强制模式。用户可以修改网络策略副本，并且为“配置 NAP 向导”创建的不符合的 NAP 客户端禁用初始网络策略。在强制模式的期限之内，配置 NAP 健康策略服务器上的强制模式。

1. 配置强制模式

① 在“网络策略服务器”管理单元中，依次展开“策略”→“网络策略”节点。双击不符合的 NAP 客户端的网络策略副本，显示“副本 NAP VPN 不符合 属性”对话框。切换至“条件”选项卡，在“条件”列表中，选择“Windows 组”选项，然后单击“删除”按钮。如图 14-118 所示。

② 切换至“设置”选项卡，在“网络访问保护”区域，选择“NAP 强制”选项，在右侧主窗口中选中“启用客户端计算机的自动更新功能”复选框，如图 14-119 所示。

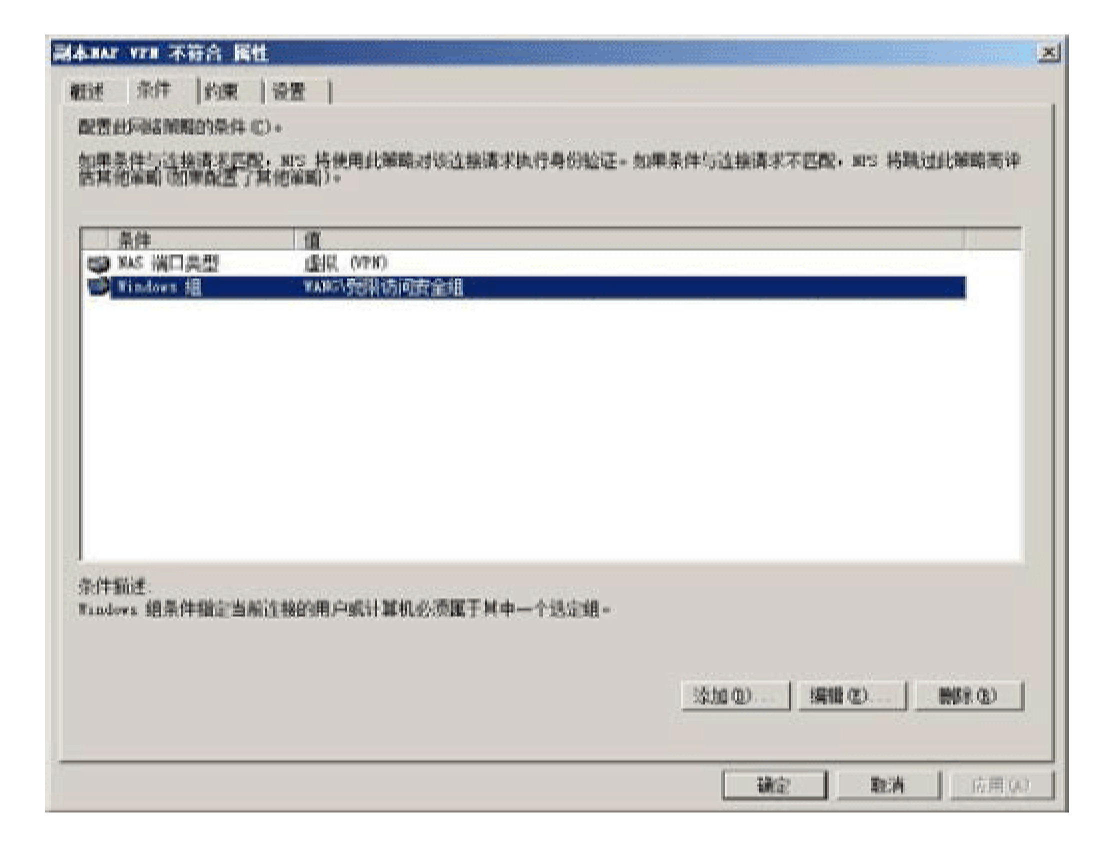


图 14-118 “条件”选项卡

图 14-119 “设置”选项卡

③ 单击“确定”按钮，保存设置。返回“网络策略”窗口，删除已经创建的不符合的 NAP 客户端的原始网络策略即可。

此时，用户用于测试不符合的 NAP 客户端的网络策略，将应用于所有 NAP 客户端上，并且删除原始的不符合的 NAP 客户端的网络策略。

2. 限制非 NAP 客户端的访问

为了限制不支持 NAP 的客户端的访问，在强制模式下，用户必须为不支持 NAP 的客户端的受限访问配置网络策略。因为不符合的 NAP 客户端的网络策略副本已经配置好，并且经过了测试，管理员可以为不支持 NAP 的客户端复制然后修改该策略。在新策略的“条件”选项卡中，单击“添加”按钮，显示“选择条件”对话框，选择“支持 NAP 的计算机”选项，单击“添加”按钮，显示“支持 NAP 的计算机”对话框，选择“仅限不支持 NAP 的计算机”单选按钮，如图 14-120 所示。

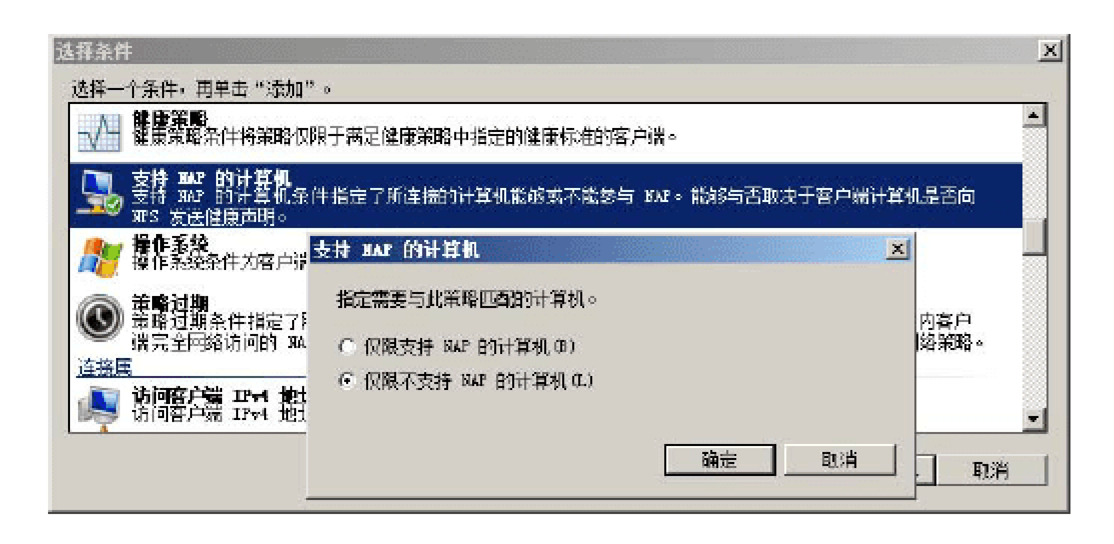


图 14-120　“选择条件”对话框

连续两次单击“确定”按钮，返回“条件”选项卡，删除原有的“健康策略”条件。在“网络策略”窗口中，将编辑后的新策略，移动到原始网络策略之上即可。

14.4　配置 DHCP 强制

NAP DHCP 强制的目的是在 DHCP 客户端租借或续订其 IP 地址时，执行客户端健康检查，根据评估结果为其分配相应作用域的 IP 地址。通常情况下，需完成下列配置。

- 在 NPS 中，配置连接请求策略、网络策略和 NAP 健康策略。可以使用 NPS 控制台单独配置这些策略，也可以使用新建网络访问保护向导。
- 在可用 NAP 的客户端计算机上启用 DHCP 强制客户端和 NAP 服务。
- 在 DHCP 控制台中，为各个作用域或在 DHCP 服务器上配置的所有作用域启用 NAP。
- 配置网络策略服务器上的 SHV。
- 配置更新服务器组。

14.4.1　配置 NAP 健康策略服务器

与配置其他强制类型的 NPS 服务器相同，首先必须安装 NPS 服务器角色，然后安装和配置 SHV。由于 NAP DHCP 强制使用的是 NPS 服务器集成的 Windows 安全健康验证程序(WSHV)，所以无须安装 SHV。

1. 配置 RADIUS 服务器设置

由于 DHCP 服务器在配置 DHCP 强制之前，不需要使用 RADIUS 验证即可分配 IPv4 地址，所以 NAP 健康策略服务器通常没有将 DHCP 服务器配置为 RADIUS 客户端。用户必须通过 NPS 管理单元添加 DHCP 服务器到 NAP 健康策略服务器上。当在“新建 RADIUS 客户端”对话框中，配置 RADIUS 客户端时，必须选中“RADIUS 客户端启用 NAP”复选框。

此外由于 DHCP 强制配置将使用报告模式，不符合的 NAP 客户端拥有不受限的访问，所以用户在启用强制模式之前可能需要更改 NAP 健康策略服务器的登录入站请求。用户可以配置 NPS 服务记录入站请求和记账信息在本地 SQL 服务器数据库文件中。

2. 为 DHCP 强制配置健康要求策略

用户可以手动或者通过“配置 NAP 向导”为 DHCP 强制创建健康要求策略。由于通过“配置 NAP 向导”进行的配置为自动完成的，所以推荐使用这种方法。

① 打开“网络策略管理器”窗口，单击 NPS，在“标准配置”下拉列表框中选择“网络访问保护(NAP)”选项。单击“配置 NAP”命令，显示如图 14-121 所示的“选择与 NAP 一起使用的网络连接方法”界面，在“网络连接方法”下拉列表中，选择“动态主机配置协议(DHCP)”，在“策略名称”文本框中，默认名称为 NAP DHCP，用户也可以自定义。

② 单击“下一步”按钮。显示如图 14-122 所示的“指定 NAP 强制服务器运行 DHCP 服务器”界面。单击“添加”按钮，即可添加符合启用 NAP 的 DHCP 服务器的 RADIUS 客户端。



图 14-121 “选择与 NAP 一起使用的网络连接方法”界面

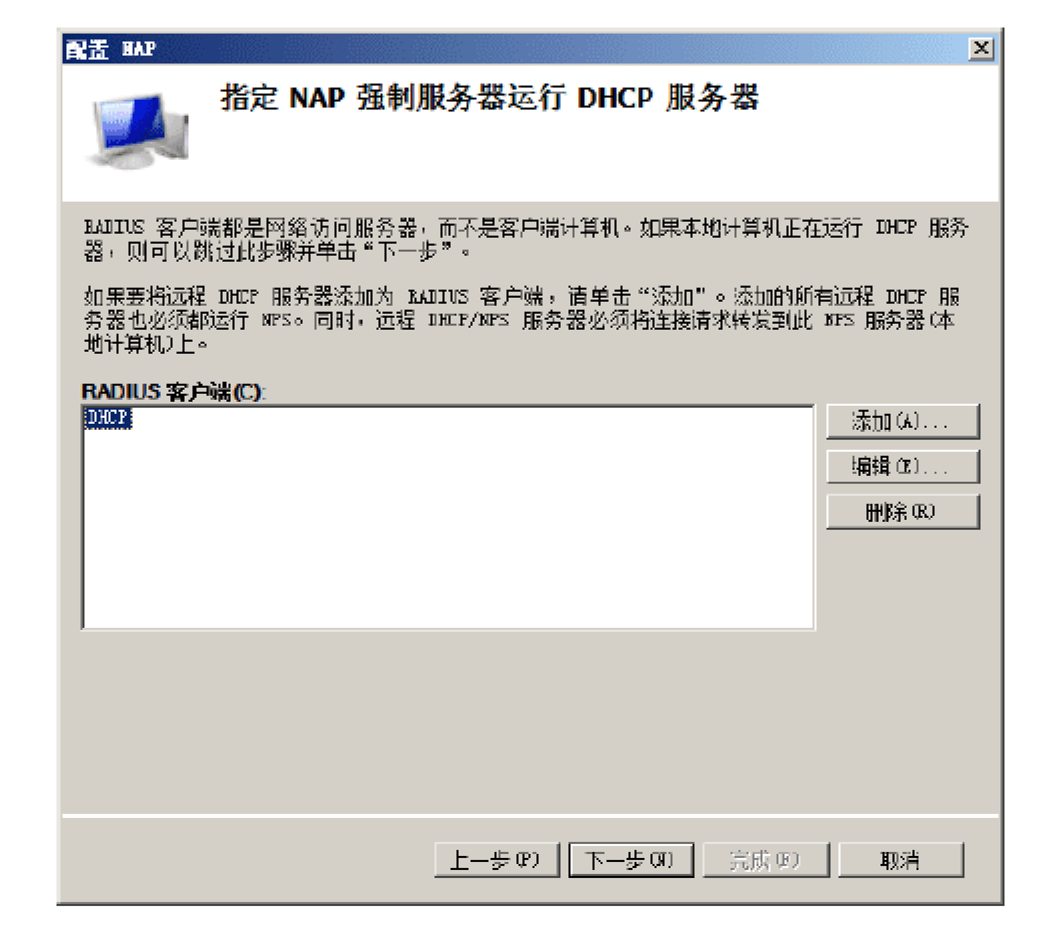


图 14-122 “指定 NAP 强制服务器运行 DHCP 服务器”界面

③ 单击“下一步”按钮，显示如图 14-123 所示的“指定 DHCP 作用域”界面，单击“添加”按钮，为健康要求策略添加标识 DHCP 作用域的配置文件名称。不管创建任何名称，都对 DHCP 服务器上的所有作用域启用 DHCP 强制。

④ 单击“下一步”按钮，显示“配置用户组和计算机组”对话框，根据需要选择计算机或组。单击“下一步”按钮，显示如图 14-124 所示的“指定 NAP 更新服务器组和 URL”界面。单击“新建组”按钮，创建新的更新服务器组，并将准备好的各种更新服务器添加到组中即可。URL 疑难解答主要用于帮助新用户认识和理解 NAP 健康策略，用户可以根据实际情况决定是否使用此项设置。

⑤ 单击“下一步”按钮，显示“定义 NAP 健康策略”对话框，选择 DHCP 强制需要评估的 SHV。选中“启用客户端计算机的自动更新”复选框，并选择“允许对不具有 NAP 功能的客户端计算机的完全网络访问权限”单选按钮，使不支持 NAP 功能的客户端拥有受限访问。因为用户想要最初的 NAP 强制模式为报告模式，所以必须选择“允许对不具有 NAP 功能的客户端计算机的完全网络访问权限”单选按钮。在配置强制模式的过程中，用户可以为不具有 NAP 功能的客户端更改网络策

略来限制访问。



图 14-123　“指定 DHCP 作用域”界面

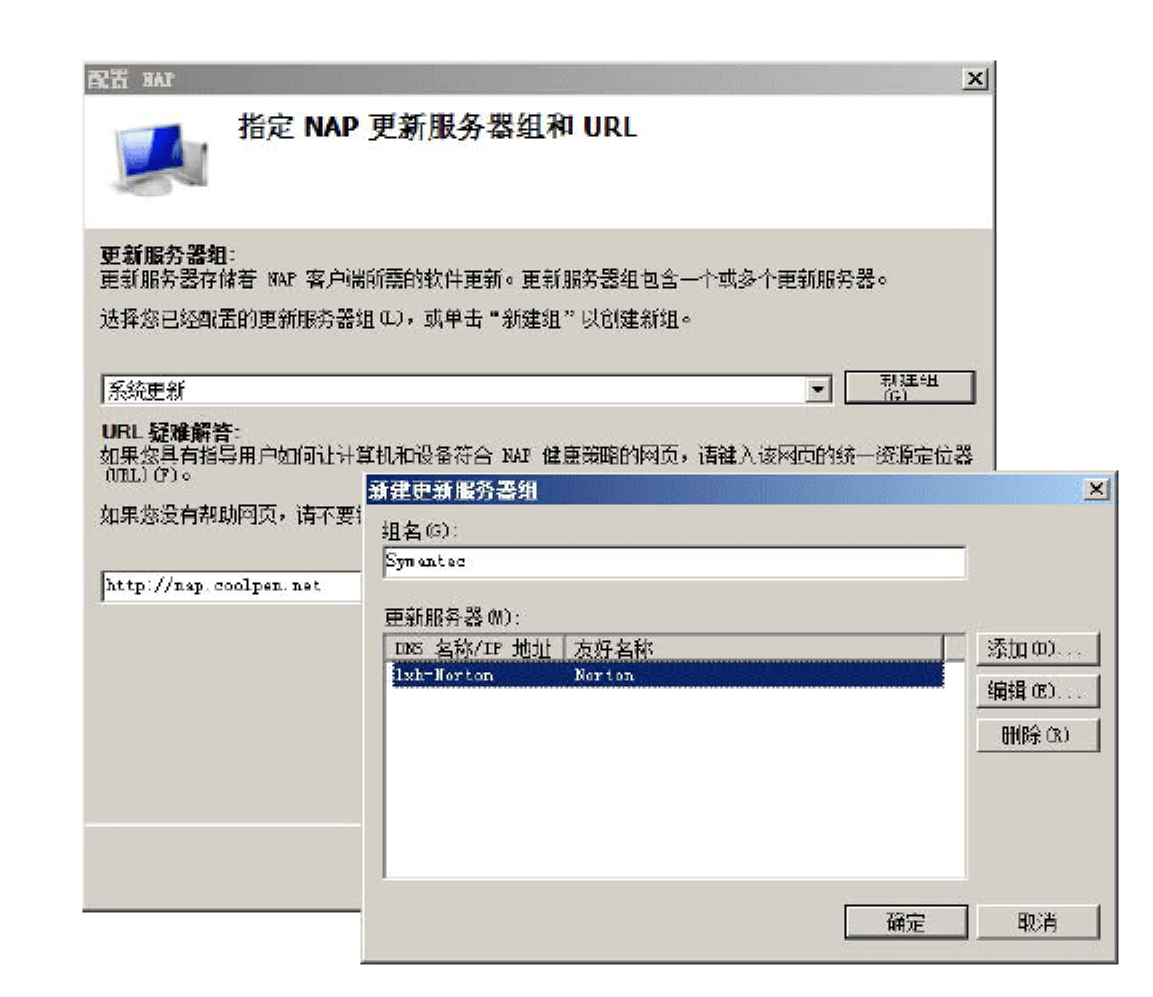


图 14-124　“指定 NAP 更新服务器组和 URL”界面

⑥　单击“下一步”按钮，显示“正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框，提示由该向导创建的各种策略以及 RADIUS 客户端和更新服务器组。

⑦　单击“完成”按钮，关闭“配置 NAP”向导。

“配置 NAP 向导”创建的连接请求策略和网络策略位于各自顺序列表的底部。由于不符合的 NAP 客户端网络策略默认情况下只允许受限访问(强制模式)，用户必须修改该策略使之允许报告模式下的不受限访问。

3. 为系统健康要求配置评估条件

①　打开“网络策略服务器”窗口，依次展开“策略”→“健康策略”节点，如图 14-125 所示。右侧栏中显示了通过配置 NAP 向导创建的健康策略，包括“NAP DHCP 符合”和“NAP DHCP 不符合”两条。

②　双击“NAP DHCP 不符合”健康策略，显示如图 14-126 所示的“NAP DHCP 不符合 属性”对话框。根据实际需要，在“客户端 SHV 检查”下拉列表框中选择相应级别的标准，如“客户端未能通过一个或多个 SHV 检查”等。“NAP DHCP 符合”健康策略的条件设置与之完全相同，此处不复赘述。

4. 允许免除安全组完全访问

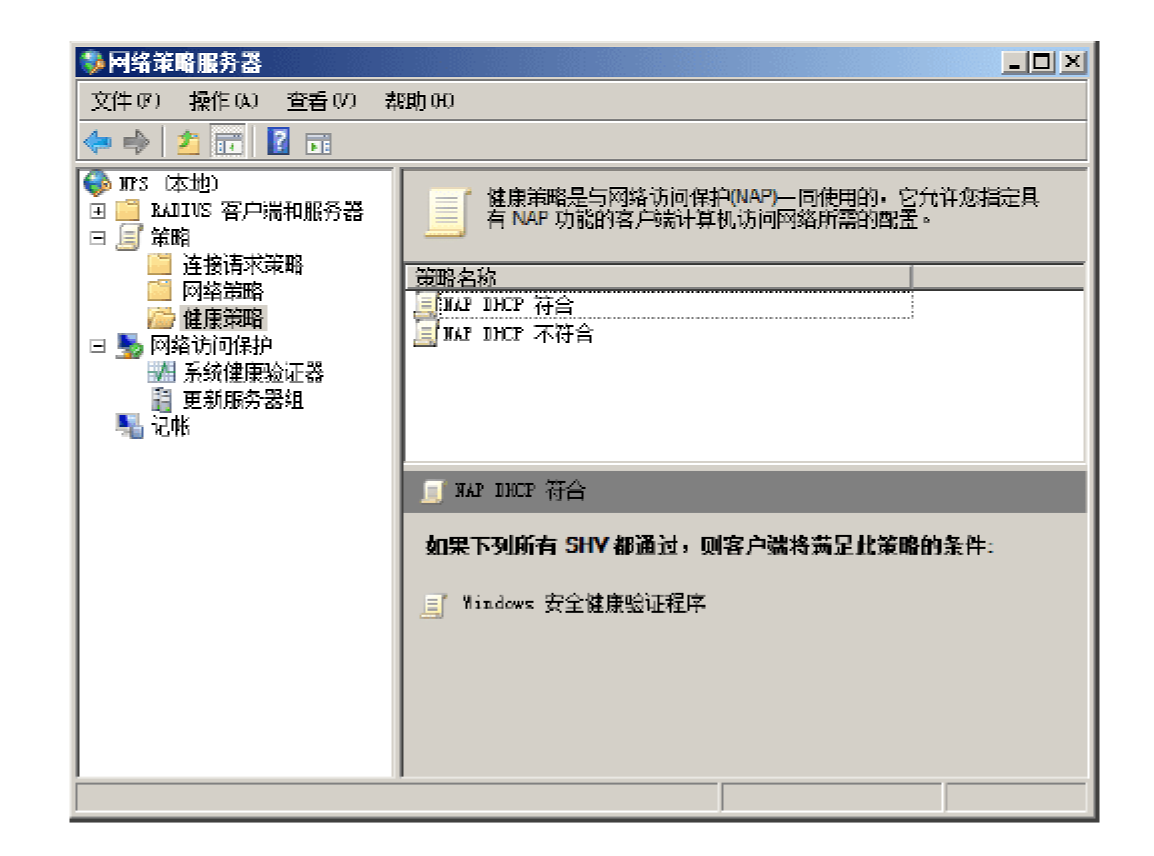
在准备工作中，已经在域中创建了免除安全组，并将需要免除的计算机添加到组中。在网络策略服务器上，必须为这些计算机创建单独的网络访问策略，使其免除 DHCP 强制。

①　打开“网络策略服务器”窗口，依次展开“策略”→“网络策略”节点。右击“配置 NAP 向导”为符合的 NAP 客户端创建 DHCP 网络策略，在弹出的快捷菜单中选择“重复策略”选项，可以看到副本，默认是禁用的，如图 14-127 所示。

②　双击“副本 NAP DHCP 符合”选项，显示如图 14-128 所示的“副本 NAP DHCP 符合 属性”对话框。在“概述”选项卡中，可以重新定义策略名称，例如“DHCP 免除安全组”。在“策略状态”区域，选中“策略已启用”复选框，并选择“授予访问权限”单选按钮。

③　切换至“条件”选项卡，单击“添加”按钮，显示“选择条件”对话框。选择“Windows 组”选项并单击“添加”按钮，显示“Windows 组”对话框，将创建好的免除安全组添加进来即可，如

图 14-129 所示。



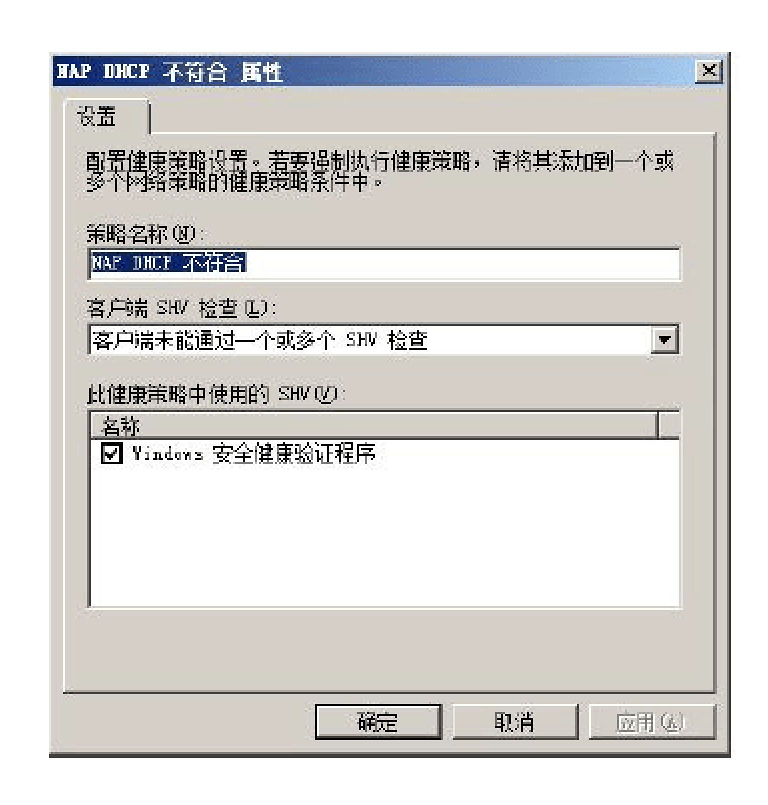
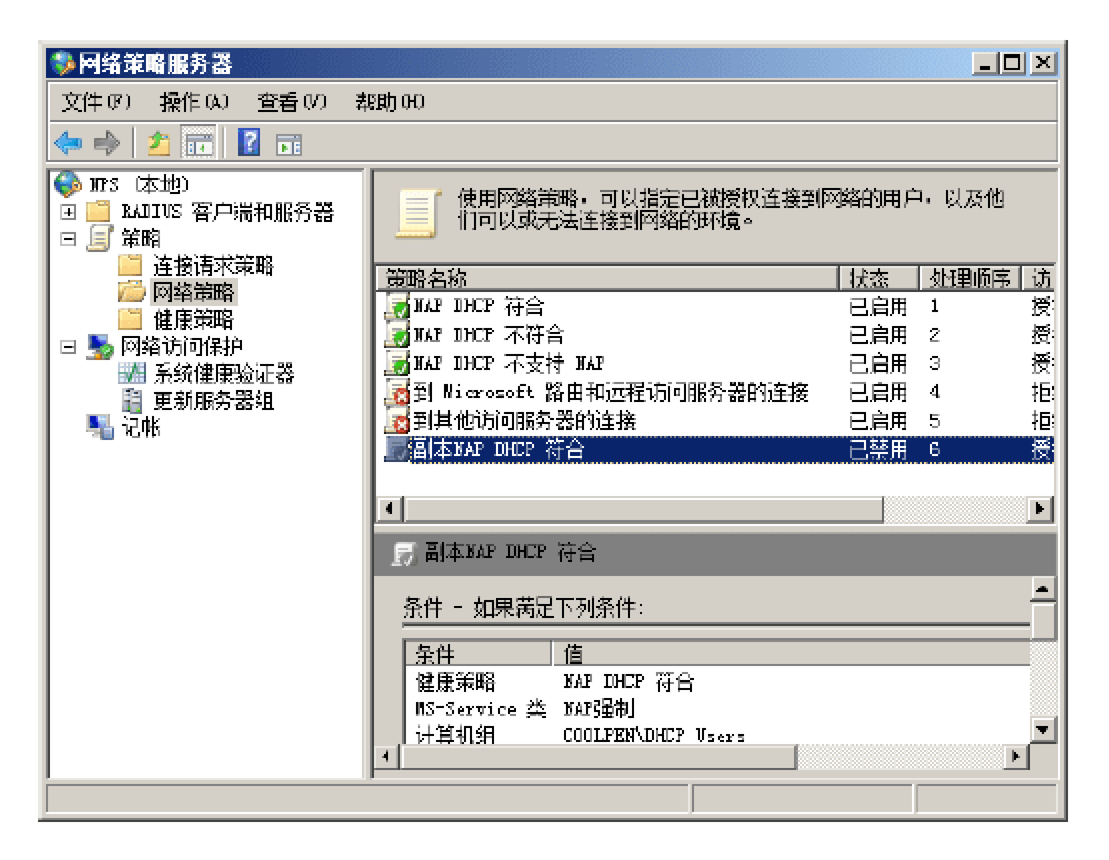


图 14-125 “网络策略服务器”窗口　　图 14-126 “NAP DHCP 不符合 属性”对话框



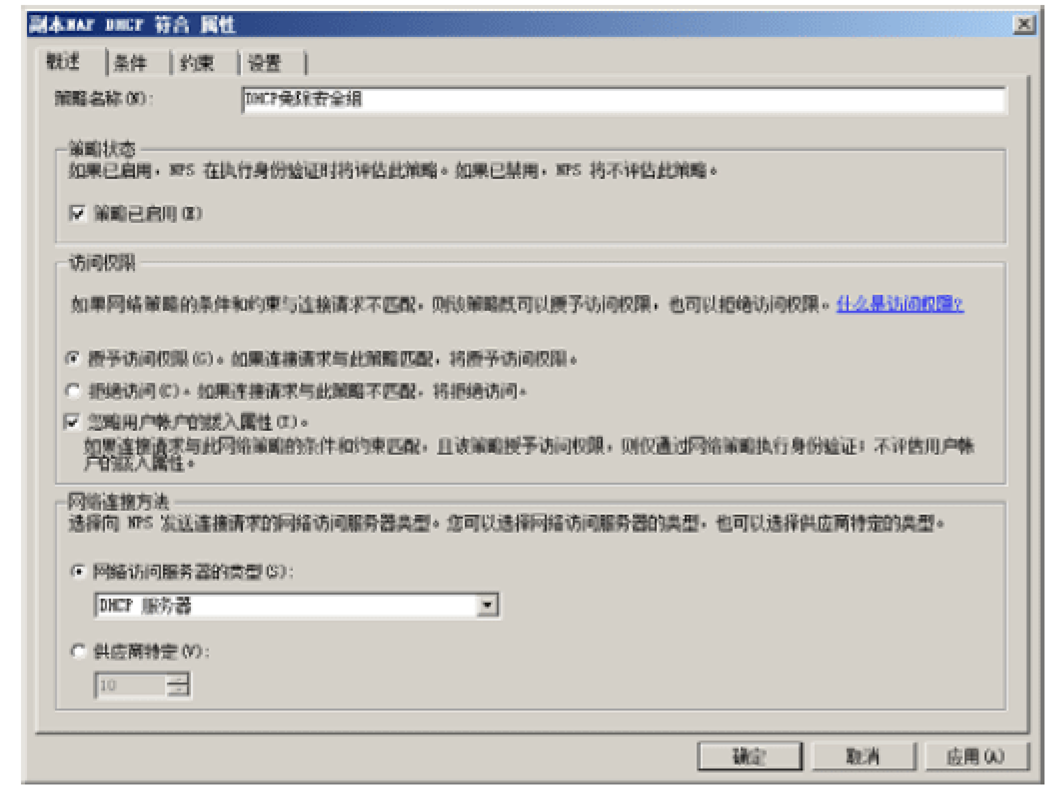


图 14-127 “网络策略服务器”窗口　　图 14-128 “副本 NAP DHCP 符合 属性”对话框

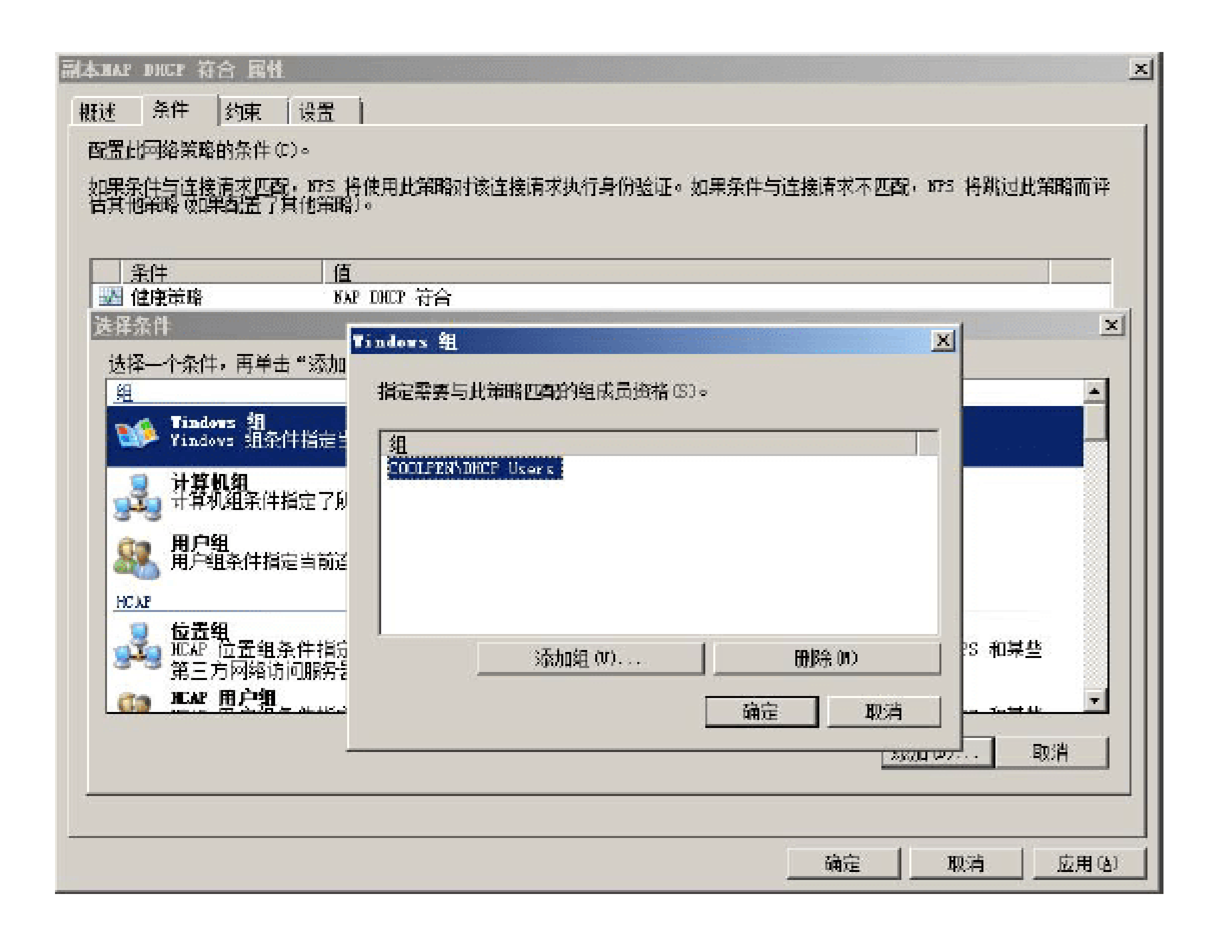


图 14-129 “条件”选项卡

④ 连续单击“确定”按钮，保存设置。同时在“条件”选项卡中删除除默认“健康策略”之外的所有条件。

⑤ 在“网络策略”窗口中，将用于免除安全组的健康策略移动到最前端，以确保对所有客户端先实施此策略评估。

14.4.2 配置 NAP 客户端

与其他类型的 NAP 客户端类似，管理员可以通过多种方式配置 NAP 客户端。如果客户端是域成员计算机，则可以借助组策略统一部署；如果是独立计算机，则可以通过修改客户端计算机的本地策略完成。主要配置操作如下。

- 配置 NAP 客户端设置
- 启用 Windows 安全中心(请参考 IPSec NAP 客户端的配置)
- 配置网络访问保护代理服务的自动启用(请参考 IPSec NAP 客户端的配置)

需要注意的是，DHCP NAP 强制客户端中需要配置的“DHCP 隔离强制客户端”，系统默认是禁用，用户只需借助组策略或其他手段，启用该功能即可，如图 14-130 所示。NAP 客户端的其他配置与 VPN 强制客户端、IPSec 强制客户端完全相同，此处不复赘述。

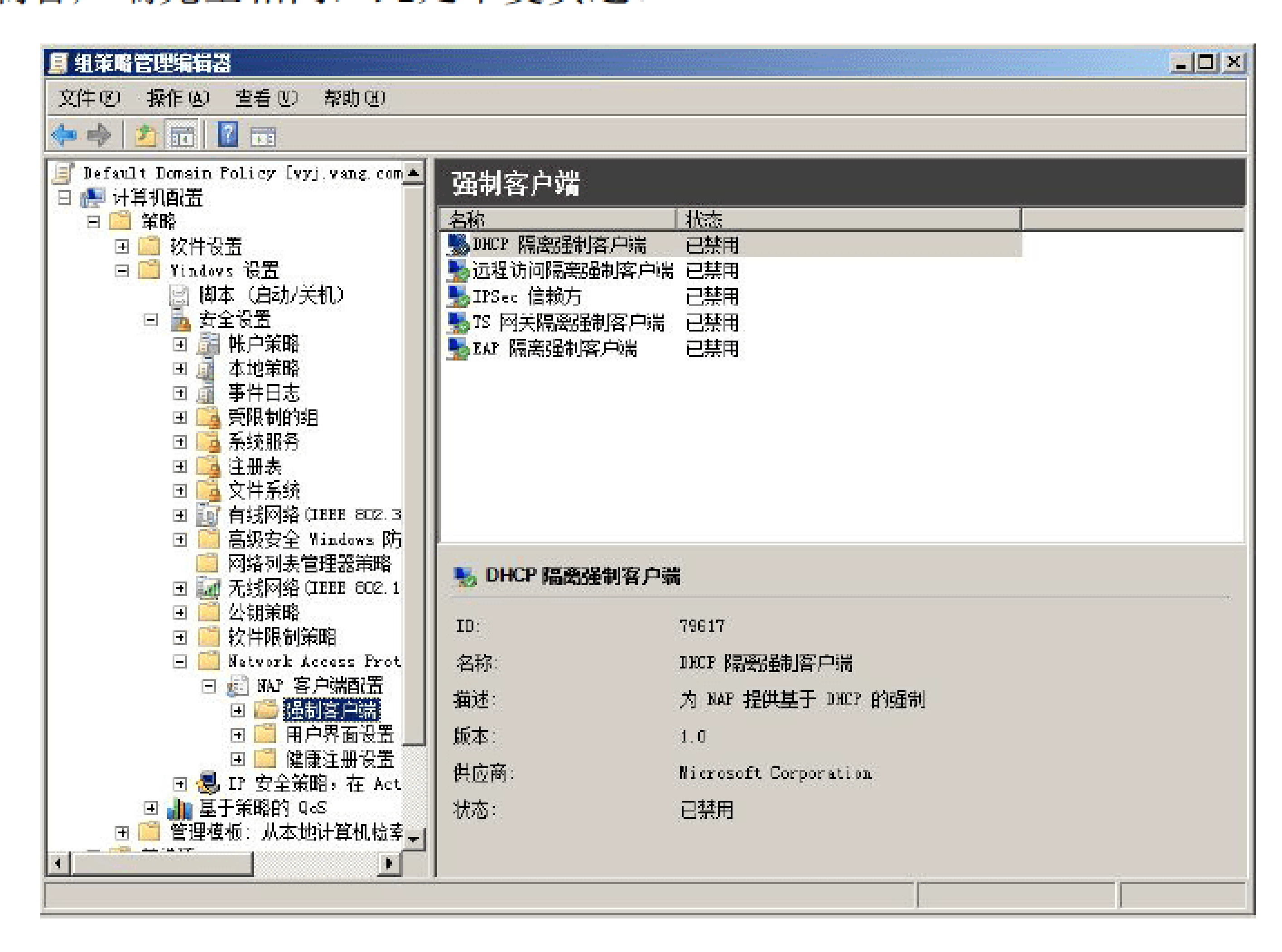


图 14-130 配置 NAP 客户端

14.4.3 将 DHCP 服务器配置为 RADIUS 客户端

NPS 服务器之所以能够响应客户端的 DHCP 请求，评估系统健康程度，原因是基于 NPS 服务器的 RADIUS 服务器，在中间起了至关重要的转发作用。因此，必须先将 DHCP 服务器配置为 RADIUS 服务器的客户端。

① 打开“网络策略服务器”窗口，依次展开“RADIUS 客户端和服务器”→“RADIUS 客户端”节点，显示如图 14-131 所示的窗口。由于在配置 NPS 服务器的网络策略时，已经将 DHCP 服务器设置为 RADIUS 客户端，所以此时并不支持 NAP。

② 右击 RADIUS 客户端，选择“属性”命令，显示如图 14-132 所示的“DHCP 属性”对话框。选中

“启用此 RADIUS 客户端”和“RADIUS 客户端支持 NAP”复选框。其他选项保持默认设置即可。

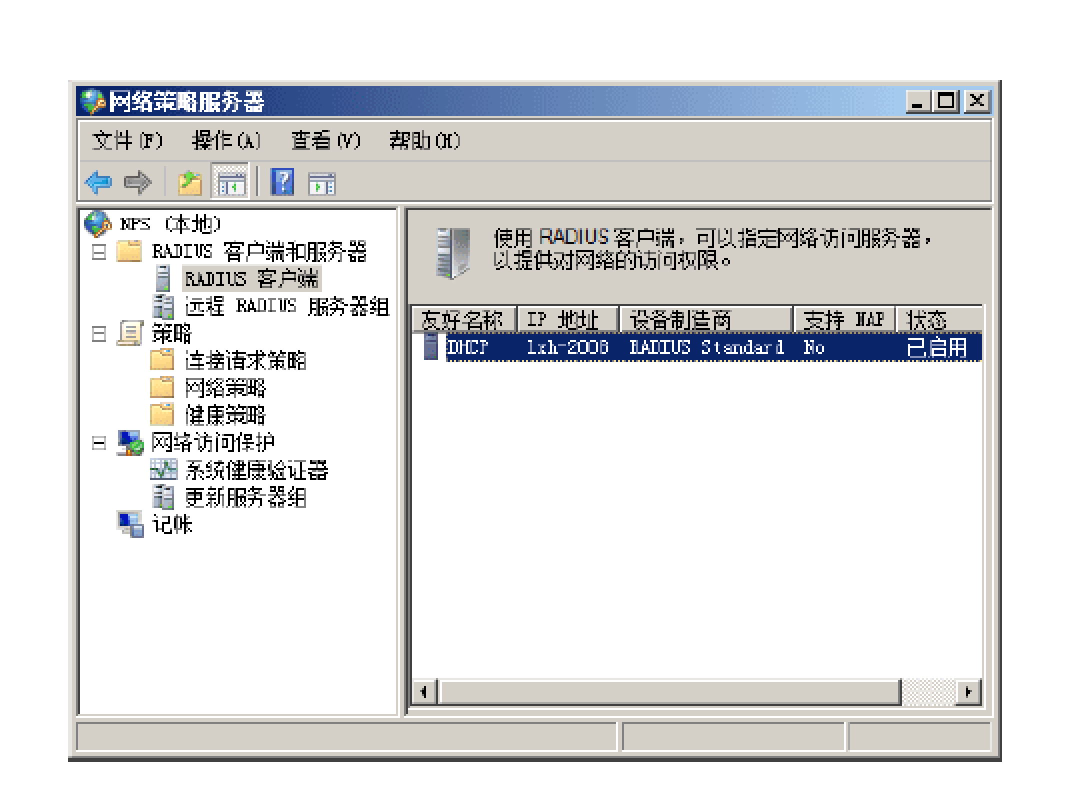


图 14-131　“网络策略服务器”窗口

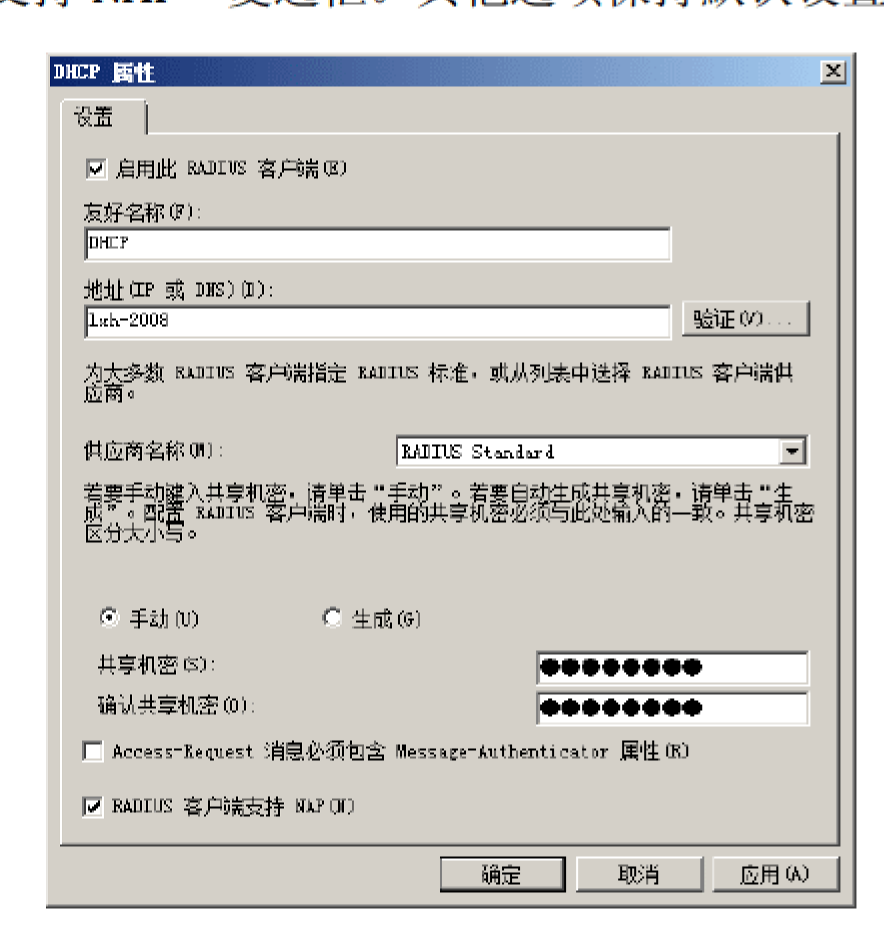


图 14-132　“DHCP 属性”对话框

14.4.4　配置 DHCP 服务器选项

当 DHCP 服务器被配置为 NPS 服务器，或者所在网络中新增 NPS 服务器后，原有 DHCP 服务将被新的包含 NPS 功能的组件所取代，管理员需要对 NPS 涉及的 DHCP 选项进行重新配置。默认状态下，NPS 关联的组件没有启用。

1. 配置作用域

NPS 安装完成后，在 DHCP 作用域属性中，添加了一项“网络访问保护”选项卡，默认情况下，该设置没有启用，需要网络管理员启用。

在 DHCP 管理窗口中，依次展开“lxh-2008.coolpen.net(服务器名称)”→IPv4 节点，显示当前 DHCP 上的所有作用域。首先，右击想要配置网络安全防护的作用域并选择“属性”命令，打开“作用域 属性”对话框，然后切换至“网络访问保护”选项卡。在“网络访问保护设置”选项区中，选择“对此作用域启用”单选按钮，如图 14-133 所示。如果在 NPS 服务器上设置了标识作用域配置文件的名称，则可以选择“使用自定义配置文件”单选按钮，并在“配置文件名”文本框中，输入指定的名称。

需要注意的是，如果此服务器同时提供 IPv6 下的 DHCP 服务，则还需要在 IPv6 的所有作用域中执行相同操作。

2. 配置服务器选项

NAP 通过新的 NAP“用户类作用域”选项，使计算机在同一作用域内的受限网络和不受限网络访问之间切换。在为状态不良的客户端计算机提供租约时，会使用这组特殊的作用域选项(DNS 服务器、DNS 域名、路由器等)。例如，提供给状态良好的客户端的默认 DNS 后缀为 coolpen.net，而给状态不良的客户端提供的 DNS 后缀为 unsafecoolpen.net。

① 在 DHCP 管理窗口中，依次展开 DHCP→“lxh-2008.coolpen.net(服务器名)”→IPv4→“服务器选项”节点，右击“服务器选项”并选择快捷菜单中的“配置选项”选项，显示如图 14-134 所示的

“服务器 选项”对话框。

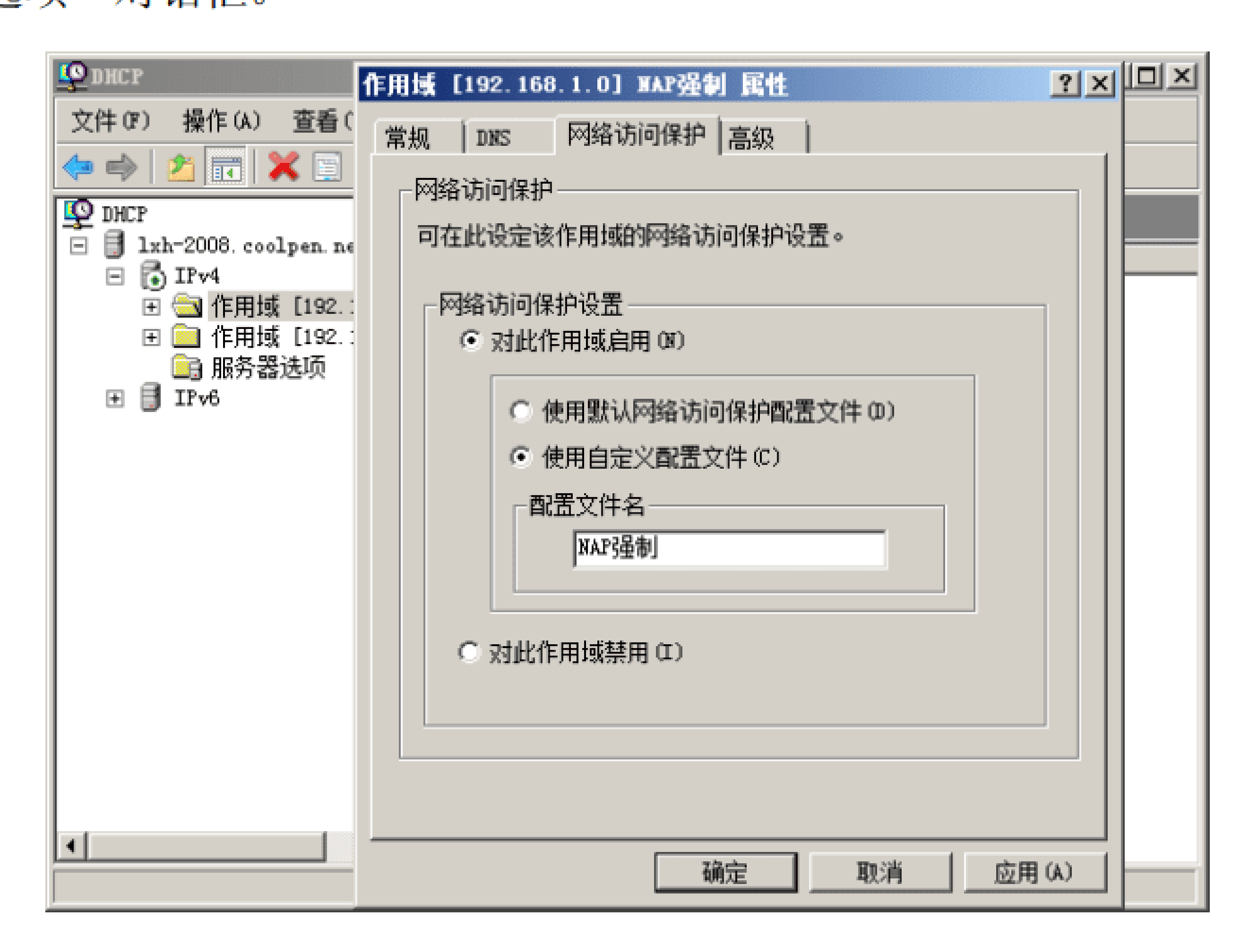


图 14-133　配置 DHCP 作用域

② 切换至“高级”选项卡，在“供应商类别”下拉列表中，选择“DHCP 标准选项”选项；在“用户类别”下拉列表框中，选择“默认的网络访问保护级别”选项，如图 14-135 所示。

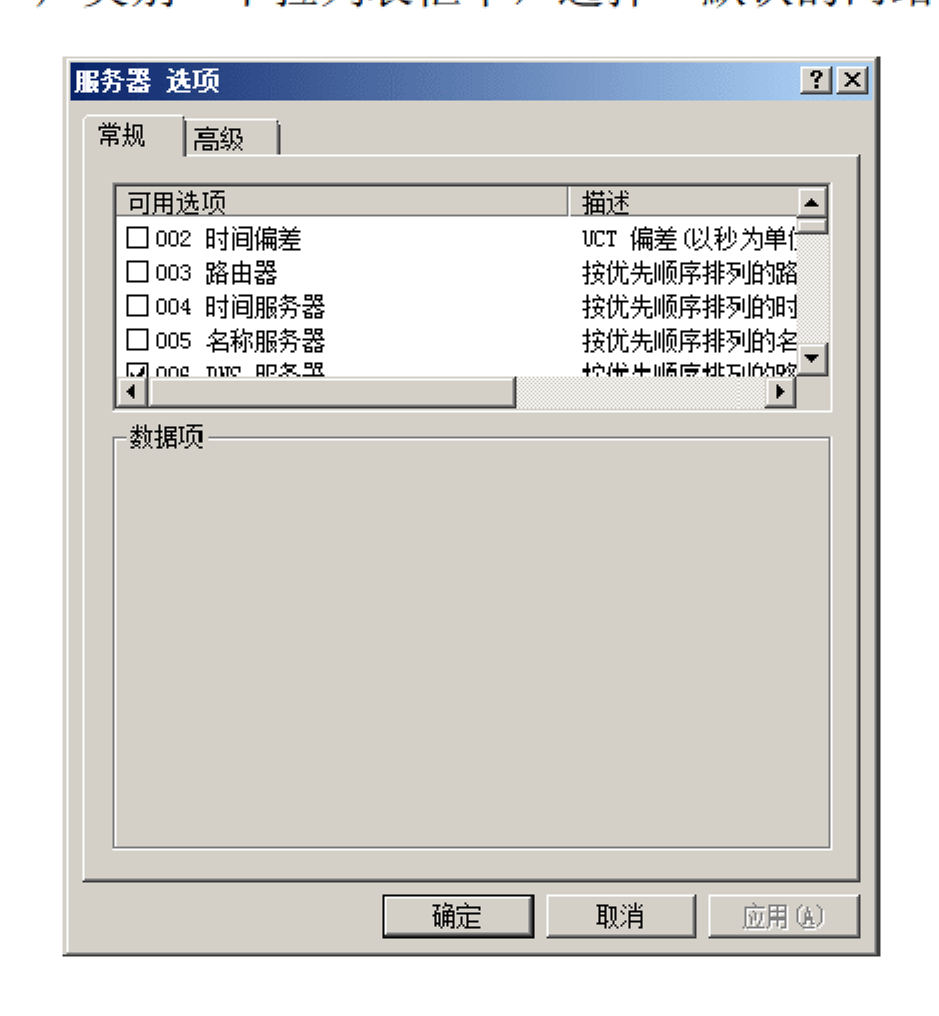


图 14-134　“服务器 选项”对话框

图 14-135　“高级”选项卡

③ 在“可用选项”列表中，选中“003 路由器”复选框，在“IP 地址”文本框中，输入网络中路由器使用的 IP 地址，例如 192.168.0.3，单击“添加”按钮。如果网络中有多个路由器，可以再次添加。如果发现路由器的顺序错误，则可以单击“向上”或者“向下”按钮，调整路由器的顺序，如图 14-136 所示。

④ 在“可用选项”列表中，选中“006 DNS 服务器”复选框，在“IP 地址”文本框中，输入网络中 DNS 服务器使用的 IP 地址，单击“添加”按钮。如果网络中有多个 DNS，可以逐次添加。如果发现 DNS 服务器的顺序错误，则可以单击“向上”或者“向下”按钮，调整 DNS 服务器的顺序，如图 14-137 所示。

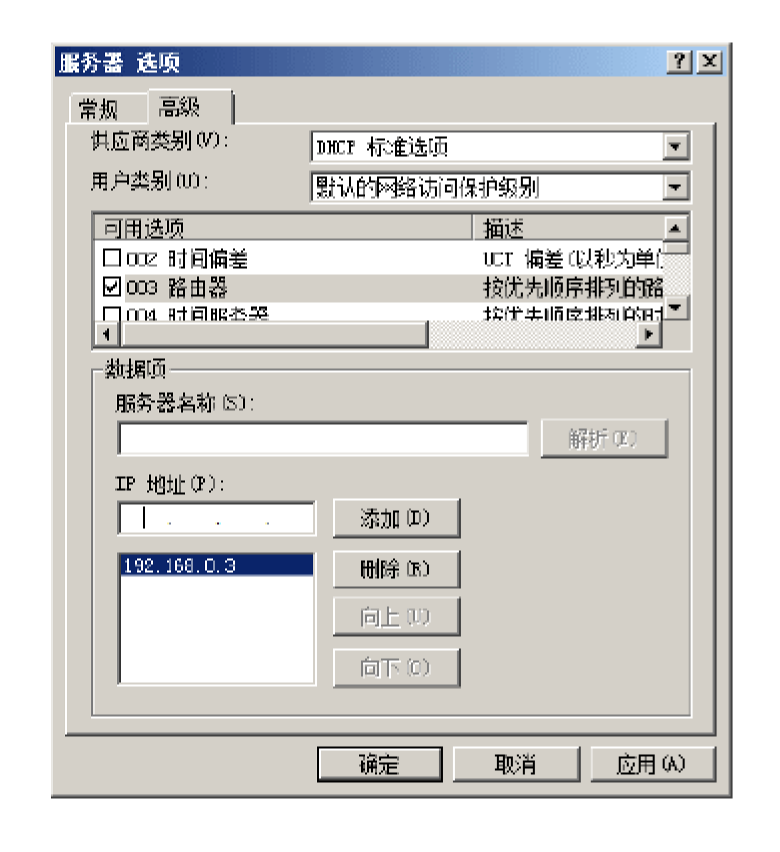
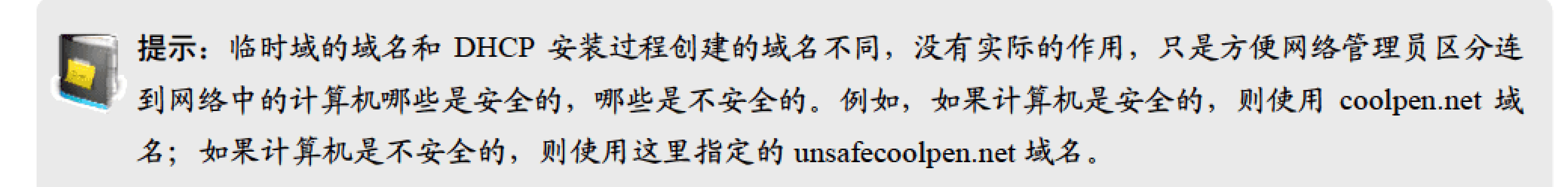



图 14-136 003 路由器



图 14-137 006 DNS 服务器

⑤ 在“可用选项”列表中，选中“015 DNS 域名”复选框，在“数据项”选项区域的“字符串值”文本框中，输入临时的 DNS 域名，如图 14-138 所示。


提示： 临时域的域名和 DHCP 安装过程创建的域名不同，没有实际的作用，只是方便网络管理员区分连到网络中的计算机哪些是安全的，哪些是不安全的。例如，如果计算机是安全的，则使用 coolpen.net 域名；如果计算机是不安全的，则使用这里指定的 unsafecoolpen.net 域名。

⑥ 单击“确定”按钮，完成服务器选项的设置，如图 14-139 所示。

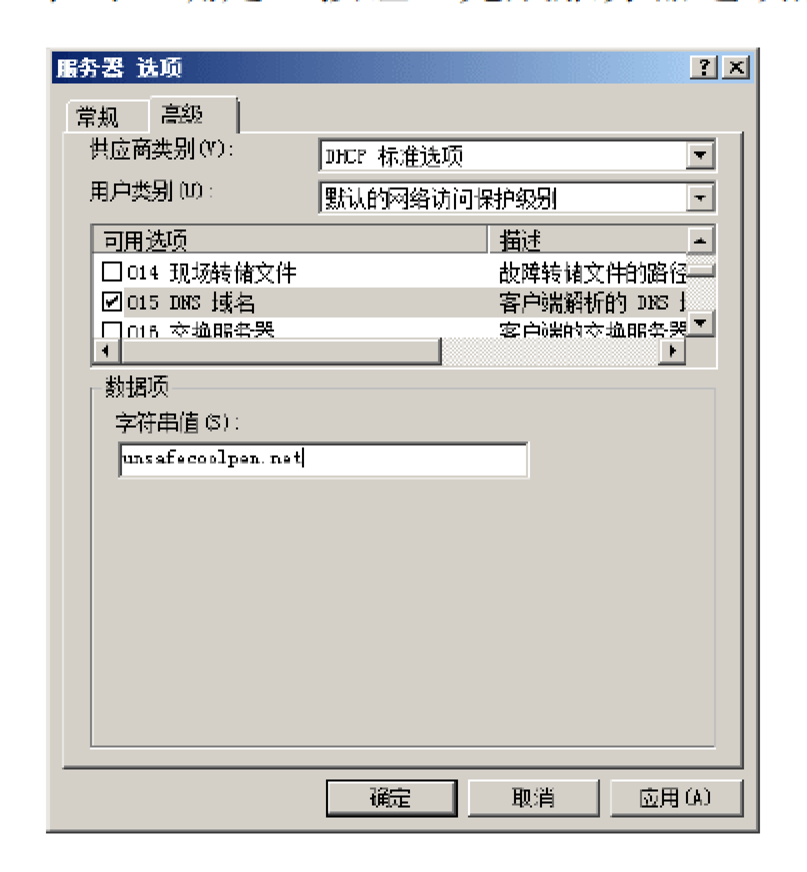


图 14-138 015 DNS 域名

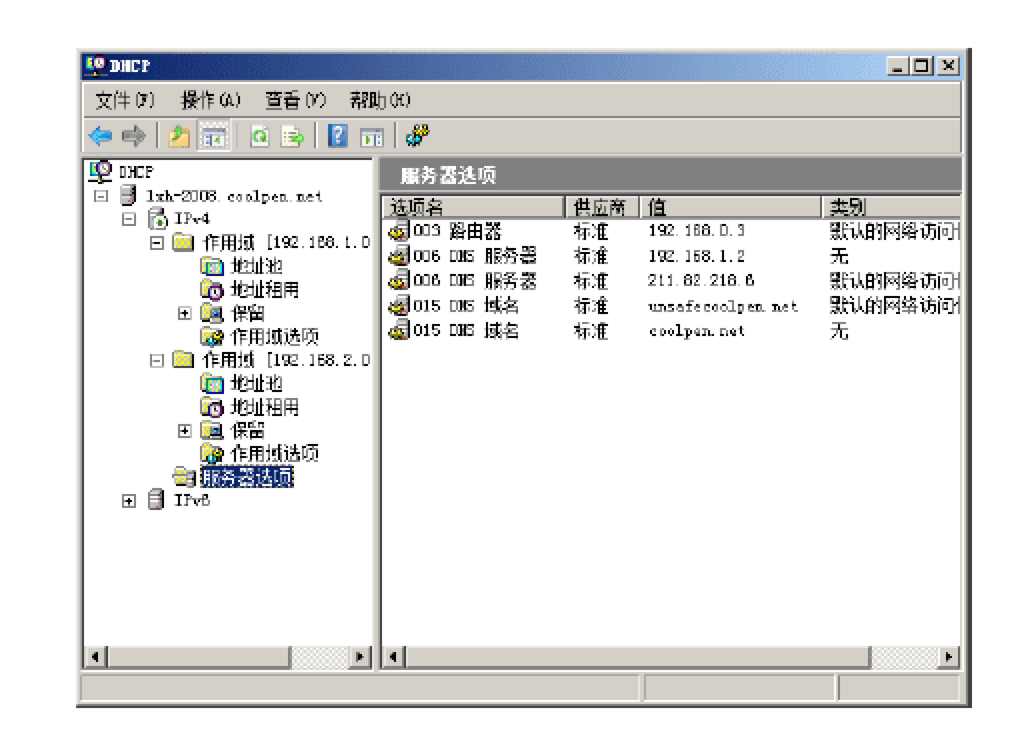


图 14-139 配置完成后的作用域选项

14.4.5 测试 DHCP 强制客户端

测试 DHCP 强制配置结果是否成功，只需在指定客户端上修改其安全配置，使其符合健康策略和不符合安全健康策略，然后查看其获取的 IP 地址类型即可。

如果客户端在关闭系统防火墙或者没有安装最新更新补丁的情况下，登录域控制器，或者登录域后关闭了某些 Windows 安全功能，则此时任务栏中会提示如图 14-140 所示的信息，提示“此计算机不符合该

网络的要求”，证明 NAP 服务器开始发挥作用。

此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 14-141 所示的“网络访问保护”对话框。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解决问题的方案。这些提示方法就是系统健康策略模板中管理员设定的处理操作。



图 14-140 不符合策略要求的客户端

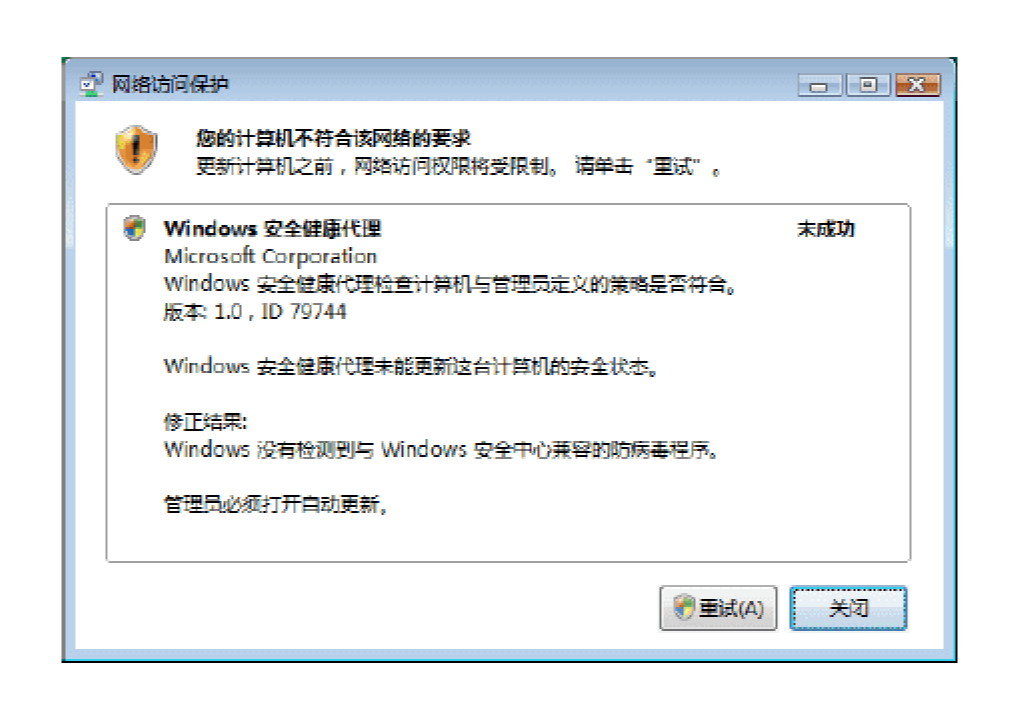


图 14-141 “网络访问保护”对话框

打开命令提示符窗口，输入 IPconfig /renew 命令，重新获取 IP 地址，再使用 ipconfig 命令，查看当前 IP 地址，显示如图 14-142 所示的结果。在 DHCP 服务器上为不安全客户端分配的 IP 地址是 192.168.2.10～192.168.2.100，而此次测试中获取的 IP 地址是 192.168.2.11，恰恰是该范围内的地址。

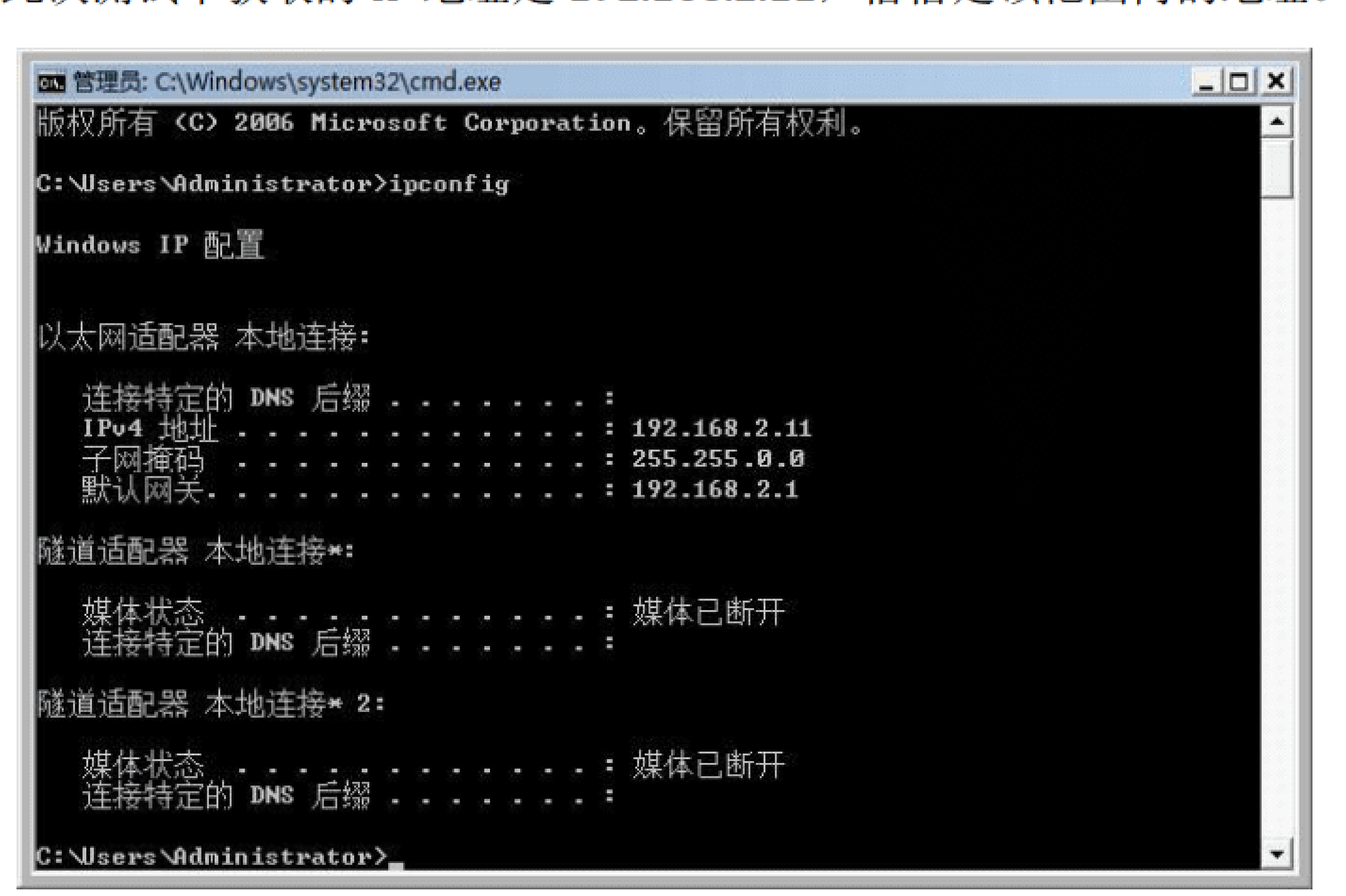


图 14-142 作为不安全客户端时获取的 IP 地址

用户可以根据提示信息尝试解决相关问题，如开启系统防火墙、恶意软件保护功能或将系统升级到最新等。处理完毕后，任务栏中会出现如图 14-143 所示的提示信息。

此时，单击“此计算机符合该网络的要求”提示信息，会显示如图 14-144 所示的“网络访问保护”对话框，可以发现已具有完全的网络访问权限。

重新获取 IP 地址，并使用 ipconfig 命令查看，显示如图 14-145 所示的结果。此次获取的 IP 地址是 192.168.1.101，与 DHCP 服务器上指定的 192.168.1.100~192.168.1.200 相符，说明 DHCP 强制配置成功。



图 14-143　符合网络策略要求

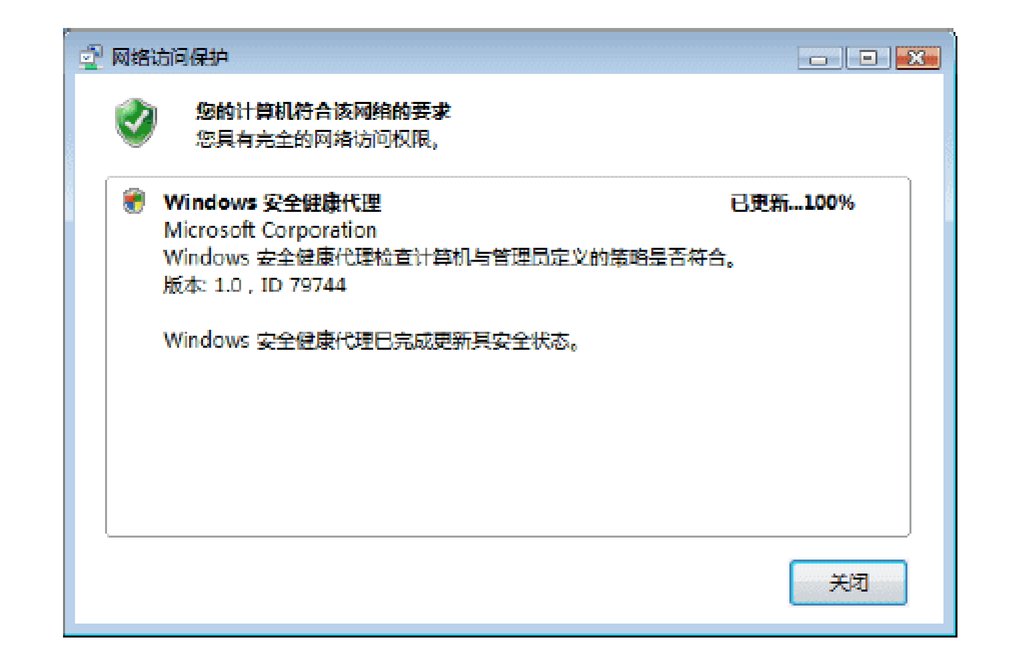


图 14-144　“网络访问保护”对话框

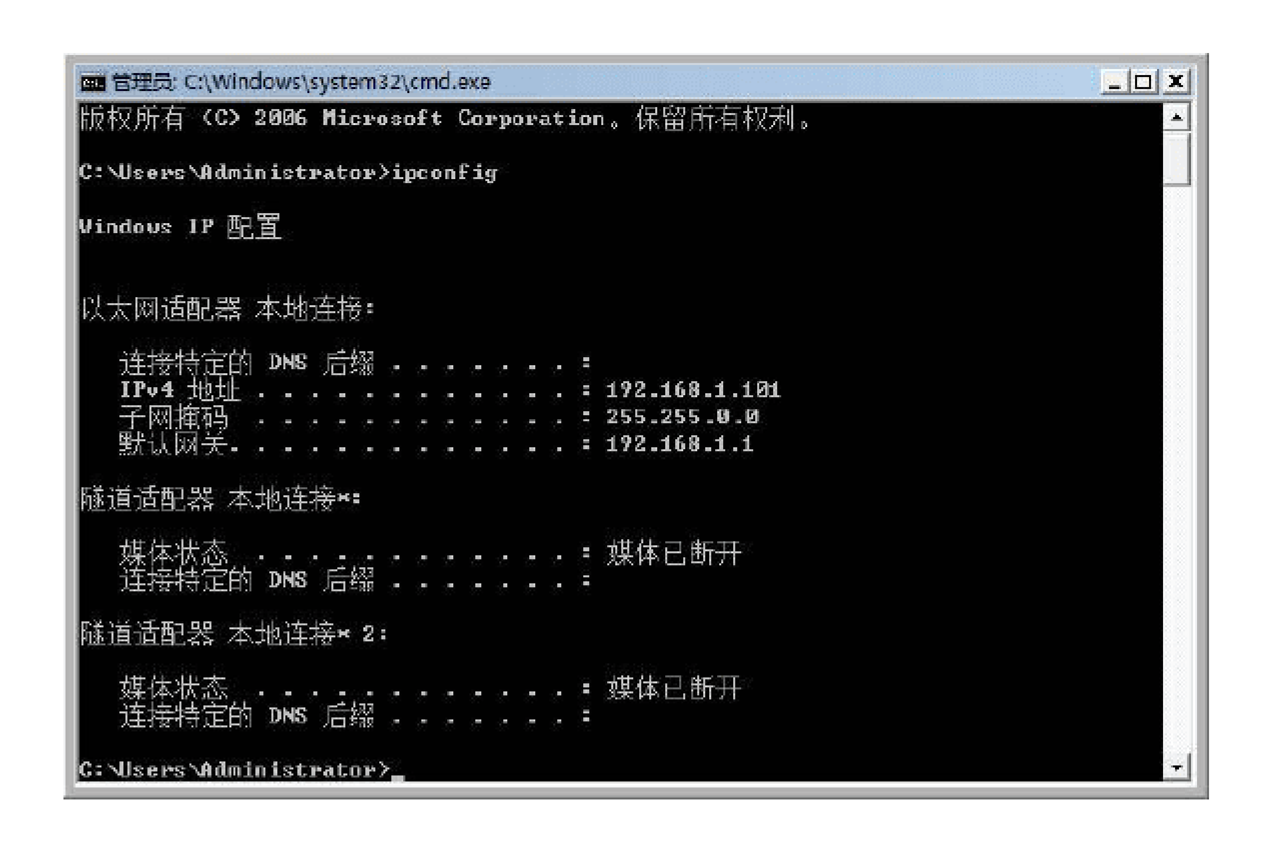


图 14-145　作为安全客户端时获取的 IP 地址

14.4.6　授权非 NAP 客户端的访问

在启用 DHCP 强制的网络中，默认是不授予非 NAP 客户端访问权限的，即网络中的类似用户将无法获取 IP 地址，也就无法访问网络。为确保此类用户能够正常获取 IP 地址，建议允许其完全访问网络。与其他强制类型配置相同，只需创建一条授权访问的网络策略，并在其评估“条件”中添加“支持 NAP 的计算机”即可。

第 15 章　数据备份与恢复

系统故障和网络攻击的发生是不可预料的。常规的系统安全措施只能起到基本的防护作用，一旦发生硬件故障或者严重的网络入侵，难免会造成数据丢失，甚至导致其死机，后果不堪设想。因此，安全管理员必需做好各种网络服务的日常备份工作。如果真的发生了重大安全故障，短时间内难以恢复，则完全可以使用备份数据快速恢复。

关键词

- 备份活动目录数据库
- 备份服务状态信息
- DHCP 服务器备份
- 磁盘配额备份
- DNS 服务器备份
- WINS 服务器备份
- 网络配置备份

15.1 备份活动目录数据库

Active Directory 是网络中所有重要信息的管理者，存储的数据包括用户账户、计算机、打印机、应用程序、安全性与系统原则等各种信息资源。因此，往往需要在网络中部署多台域控制器，一方面可以相互分担网络负载，更重要的是可以互为备份，例如，额外域控制器等。其实，仅实施这些方案是完全不够的，最安全的方法就是定期对活动目录数据库进行离线备份，并妥善保管存储备份的服务器或存储介质，以备恢复时使用。

15.1.1 活动目录数据库的备份

活动目录数据库的数据量虽然不像文件服务器那样巨大，但却十分重要，存储着网络上所有用户账户以及计算机等网络资源的信息，尤其是在单域控制器的网络中，其重要性更为突出。百密难免一疏，没有绝对安全的系统和硬件，最好的方法就是防患于未然。对于活动目录数据库而言，就是时刻做好备份工作，如果条件允许还可以多制作几份备份，提高安全性。万一发生严重故障，导致数据丢失或损坏，可以方便地从备份中还原该数据。

1. 备份功能

备份活动目录可以完成以下数据状态的迁移。

- 在硬盘上选择存档的文件和文件夹。
- 将存档文件和文件夹还原到硬盘或其他任何可以访问的磁盘上。
- 使用“自动系统故障恢复”可以保存和还原系统故障中所恢复的所有系统文件和配置设置。
- 复制所有远程存储数据和所有存储在已装入的驱动器中的数据。
- 为所在计算机的系统状态制作副本。
- 创建日志，记录所备份的文件以及备份的时间。
- 备份计算机在此计算机或网络发生故障时启动系统所需的系统分区、启动分区和文件。
- 计划并定期备份，保持存档数据是最新的。
- “备份”还可以执行简单的媒体管理功能，如格式化。更高级的管理任务(如装载和卸载磁带或磁盘等)将由称为“可移动存储”的服务来完成。

2. Windows Server Backup

Windows Server Backup 是 Windows Server 2008 系统的新增功能之一，取代了原 Windows 系统中的附带的备份功能(Ntbackup.exe)。Windows Server Backup 可以为用户的日常备份和恢复提供更为完整的方案和计划，既可以备份整个服务器(所有卷)的数据，也可以只备份用户选择的卷或状态信息，应用非常方便。

(1) 新增功能

相对先前 Windows 系统中的备份和还原工具，Windows Server Backup 包括如下改进。

- 速度更快。Windows Server Backup 使用卷影复制服务(VSS)和块级别的备份技术，对系统数据和服务器数据进行备份。用户只需第一次创建一个完整的备份，接下来执行 Windows Server Backup

的增量备份功能，即可快速完成完整备份，所需时间更少，效率更高。

- 操作简单。无论是数据库备份、还原还是制定备份计划，完全在向导指引下完成，操作更加简便。另外，用户还可以从备份中选择需要恢复的单个项目进行操作，而不必进行全面恢复，既节约时间又可以避免不必要的数据覆盖。
- 系统恢复更简单。Windows Server Backup 与新的 Windows 恢复工具配合使用，使操作系统恢复更加简单，而且还可以使用副本，对其他类似硬件配置的服务器进行系统恢复(通常为未安装任何系统的全新计算机)。
- 恢复应用程序。Windows Server Backup 可以使用内置到应用程序中的 VSS 功能来保护应用程序数据。
- 非现场删除备份以便进行灾难保护。Windows Server Backup 可以将备份轮流保存到多个磁盘中，这样使管理员可以在非现场位置移动磁盘，将每个磁盘添加为一个计划备份的位置。如果第一个磁盘不在现场，则 Windows Server Backup 会自动将备份顺序保存到下一个磁盘中。
- 远程管理。Windows Server Backup 是基于 MMC 控制台的，管理员可以将它轻松连接至另一台远程计算机上，实现远程控制。
- 自动磁盘使用情况管理。在实施备份计划时，Windows Server Backup 会自动检查磁盘的使用情况，如果剩余空间不足，将自动重复使用陈旧备份的空间。
- 扩展命令行支持。Windows Server Backup 包含 Wbadmin 命令和文档，管理员可以在命令提示符窗口中执行备份和恢复任务。
- 支持光学存储介质。Windows Server Backup 允许管理员通过手动方式，将卷直接备份到光盘或其他可移动存储介质上。

(2) 安装 Windows Server Backup

Windows Server Backup 是 Windows Server 2008 中唯一的备份工具，备份活动目录数据库时，需要用到其中的命令行工具。该命令行工具只能随同 Windows Server Backup 一起安装，位于“服务器管理器”的“添加功能”向导中。安装步骤如下。

① 依次选择“开始”→“管理工具”→“服务器管理器”命令，打开“服务器管理器”窗口并展开“功能”，单击“添加功能”命令，显示如图 15-1 所示的“添加功能向导”对话框。在“功能”列表框中选中“Windows Server Backup 功能”复选框即可。系统默认不会选中“命令行工具”复选框，如果手动选中，将显示如图 15-2 所示的“是否添加 命令行工具 所需的功能”界面。

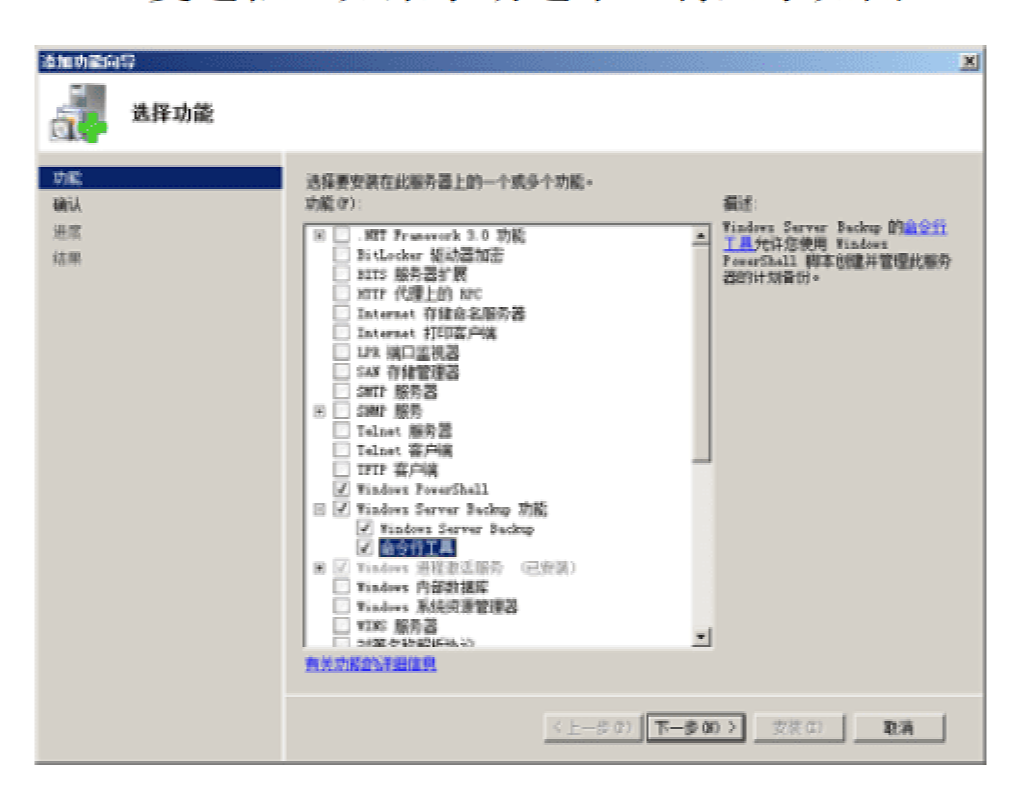


图 15-1　“添加功能向导”对话框



图 15-2　“是否添加 命令行工具 所需的功能”界面

> **提示：**“命令行工具”允许管理员使用 Windows PowerShell 脚本，创建并管理此服务器的计划备份以及高级还原模式。对于域控制器而言必须选择此组件，否则无法进行活动目录数据库的还原，普通用户建议使用 UI 界面即可。

② 单击“下一步”按钮，显示如图 15-3 所示的“确认安装选择”界面，列表框中显示了前面选择的要安装的功能。

③ 单击“安装”按钮开始安装。完成后显示如图 15-4 所示的“安装结果”界面。

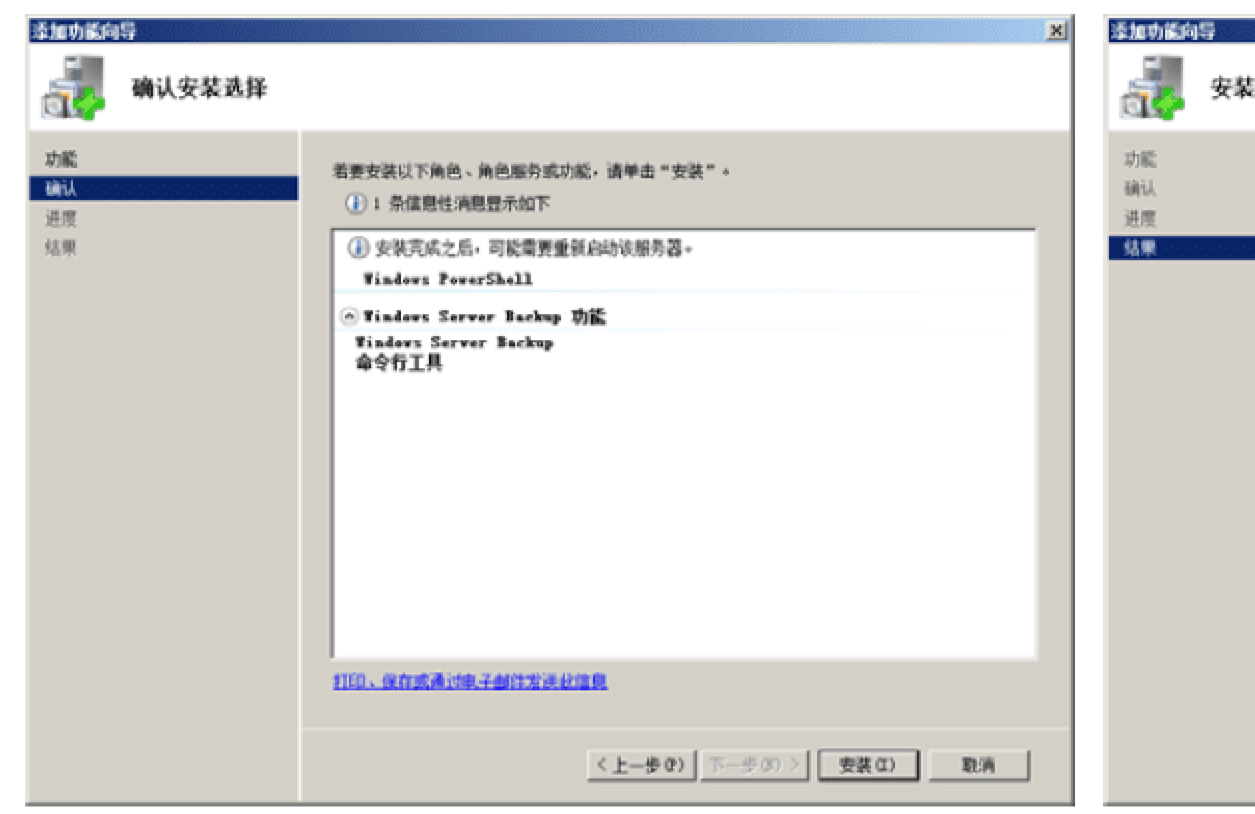


图 15-3 “确认安装选择”界面



图 15-4 “安装结果”界面

④ 单击“关闭”按钮，退出安装向导，完成 Windows Server Backup 功能的安装。

3. 备份活动目录数据库

Windows Server Backup 备份向导，可以帮助用户快速备份磁盘分区和所有系统数据，但无法用来单独备份 Active Directory 目录数据库，即系统状态信息。Wbadmin 命令行备份为网络管理员提供自由的备份模式，主要功能就是备份 Active Directory 服务器的系统状态，在域控制器工作过程中即可完成。主要操作步骤如下。

① 以具有管理员权限的用户账户登录服务器，依次选择“开始”→“命令提示符”命令，打开“管理员：命令提示符”窗口。直接输入“wbadmin”命令并按 Enter 键，即可查看其帮助信息，如图 15-5 所示。

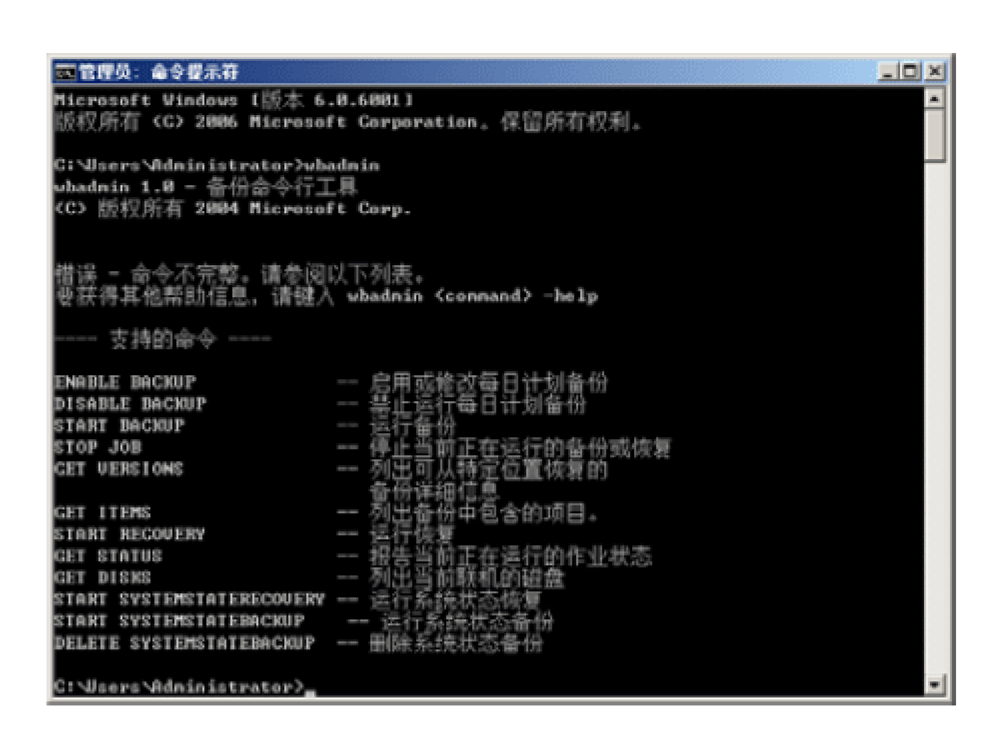


图 15-5 wbadmin 命令帮助信息

② 输入如下命令：

```
Wbadmin get disks
```

按 Enter 键运行，查看当前服务器连接到的磁盘，即所有磁盘分区，显示如图 15-6 所示的结果。

③ 输入如下命令：

```
wbadmin START SYSTEMSTATEBACKUP -backuptarget:d:
```

按 Enter 键，显示如图 15-7 所示的结果，将系统状态信息备份到 D 盘根目录下。管理员只需指定目标分区即可，备份向导将自动根据当前系统日期和时间，命名备份文件，以便日后区分。

```
管理员: 命令提示符
C:\Users\Administrator>wbadmin get disks
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.

磁盘名称        : VMware, VMware Virtual S SCSI Disk Device
磁盘数量        : 0
磁盘标识符      : {b6cdbeeb-0000-0000-0000-000000000000}
总空间          : 41.00 GB
已用空间        : 8.77 GB
卷              : C:[(没有卷标签)],D:[(没有卷标签)]

磁盘名称        : VMware, VMware Virtual S SCSI Disk Device
磁盘数量        : 1
磁盘标识符      : {2ab5e863-0000-0000-0000-000000000000}
总空间          : 40.00 GB
已用空间        : 7.97 GB
卷              : F:[Backup]

C:\Users\Administrator>
```

图 15-6　检查已连接的磁盘



图 15-7　备份系统状态信息

④ 系统提示是否需要创建备份卷的卷影副本，输入“y”(或“是”)并按 Enter 键，开始收集关联文件，如图 15-8 所示。文件收集完成后，将自动开始执行备份过程。

⑤ 备份完成后，显示如图 15-9 所示的窗口。

```
管理员: 命令提示符 - wbadmin START SYSTEMSTATEBACKUP -backuptarget:d:
C:\Users\Administrator>wbadmin START SYSTEMSTATEBACKUP -backuptarget:d:
wbadmin 1.0 - 备份命令行工具
(C) 版权所有 2004 Microsoft Corp.

开始系统状态备份[2008/6/1 16:48]
正在检索卷信息...

这会将系统状态从卷 本地磁盘(C:) 备份到卷 d:。
是否要开始备份操作?
[Y] 是 [N] 否 y

创建请求备份的卷的卷影副本。
创建请求备份的卷的卷影副本。
创建请求备份的卷的卷影副本。
正在识别要备份的系统状态文件(这可能需要几分钟时间)...
找到(306)文件
找到(1120)文件
找到(1787)文件
找到(2690)文件
找到(3901)文件
找到(4798)文件
找到(5899)文件
找到(7346)文件
找到(8455)文件
```

图 15-8　开始收集关联文件

```
管理员: 命令提示符
总体进度 - 95% (当前正在备份由“System Writer”报告的文件)
总体进度 - 96% (当前正在备份由“System Writer”报告的文件)
总体进度 - 97% (当前正在备份由“System Writer”报告的文件)
总体进度 - 97% (当前正在备份由“System Writer”报告的文件)
备份由“System Writer”报告的文件已完成
备份由“WMI Writer”报告的文件已完成
备份由“COM+ REGDB Writer”报告的文件已完成
备份由“FRS Writer”报告的文件已完成
备份由“IIS Config Writer”报告的文件已完成
总体进度 - 98% (当前正在备份由“Registry Writer”报告的文件)
备份由“Registry Writer”报告的文件已完成
备份由“NTDS”报告的文件已完成
总体进度 - 99% (当前正在备份附加系统状态文件)

备份摘要:
------------------

系统状态备份成功完成[2008/6/1 17:12]

成功备份文件日志
“C:\Windows\Logs\WindowsServerBackup\SystemStateBackup 01-06-2008 16-49-02.log
”

C:\Users\Administrator>
```

图 15-9　备份完成

⑥ 关闭“管理员：命令提示符”窗口，建议重新启动计算机，因为数据库备份必须在重新启动之后方可应用。

15.1.2　活动目录数据库的恢复

域控制器的数据库损坏或数据丢失，将直接影响到网络功能的提供，尤其是在单域网络环境中，活动

目录数据库的备份显得更为重要。如果仅是数据库故障，则直接使用备份文件恢复数据库即可。需要注意的是，活动目录数据库的恢复，需要在“目录服务还原模式”下完成，主要操作步骤如下。

① 在启动域控制器时，按 F8 键启动到“高级启动选项”画面，如图 15-10 所示。只有安装 Windows Server Backup 中的命令行工具后，启动菜单中才会出现“目录服务还原模式”选项。

② 选择“目录服务还原模式”并按 Enter 键，开始启动系统。注意，必须以本地系统管理员账户登录系统，如图 15-11 所示。此时的域控制器是不可用的。



图 15-10 “高级启动选项”画面

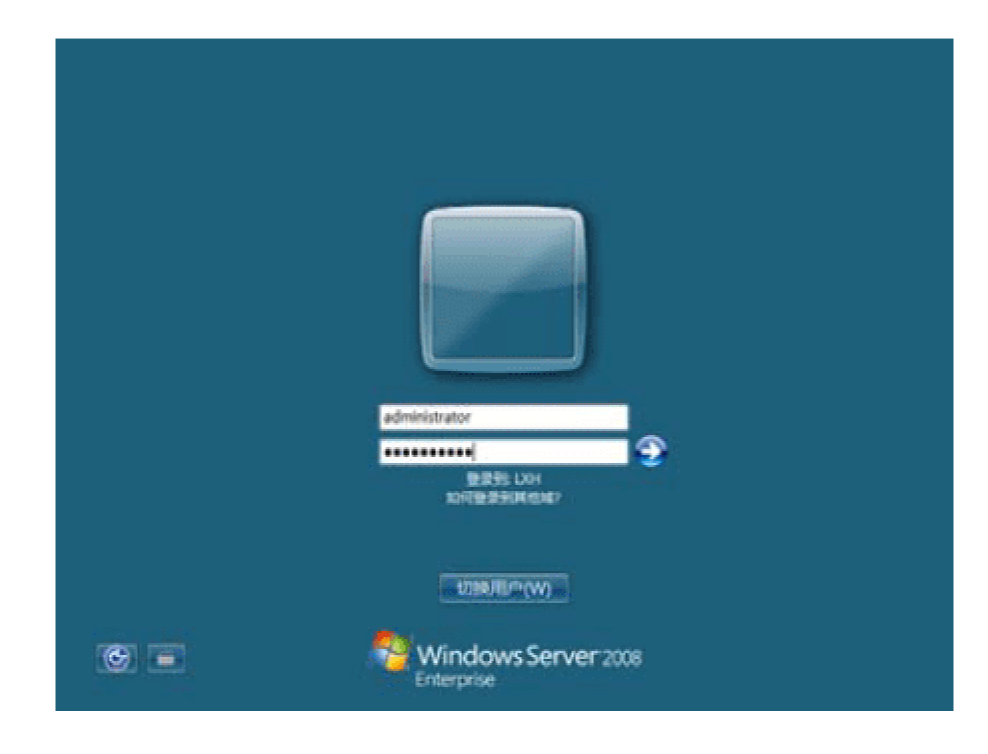


图 15-11 登录系统

③ 启动到 Windows 安全模式后，打开“命令提示符”窗口，输入如下命令：

```
wbadmin get versions
```

按 Enter 键，显示如图 15-12 所示的结果。恢复目录数据库时是通过每次备份的版本信息确定的，默认格式为 mm/dd/yyyy-hh:mm，如 06/01/2008-08:49。

④ 继续输入如下命令：

```
wbadmin start systemstaterecovery -version: 06/01/2008-08:49
```

按 Enter 键，显示如图 15-13 所示的结果，提示网络管理员是否要执行系统状态恢复。

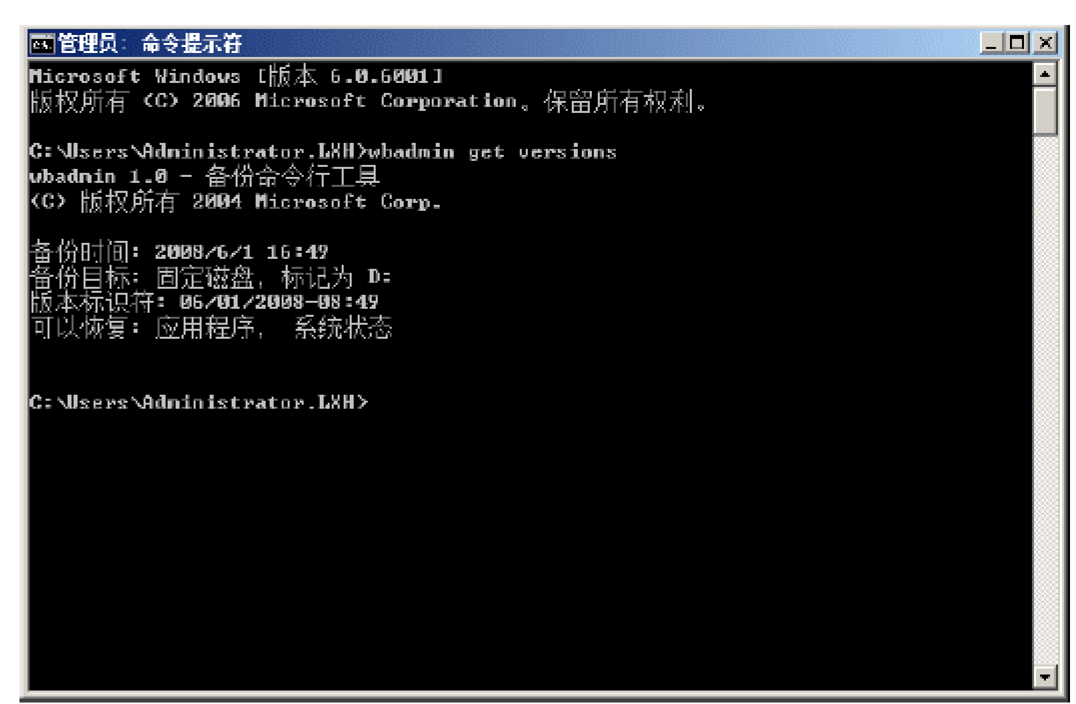


图 15-12 查看备份版本标识

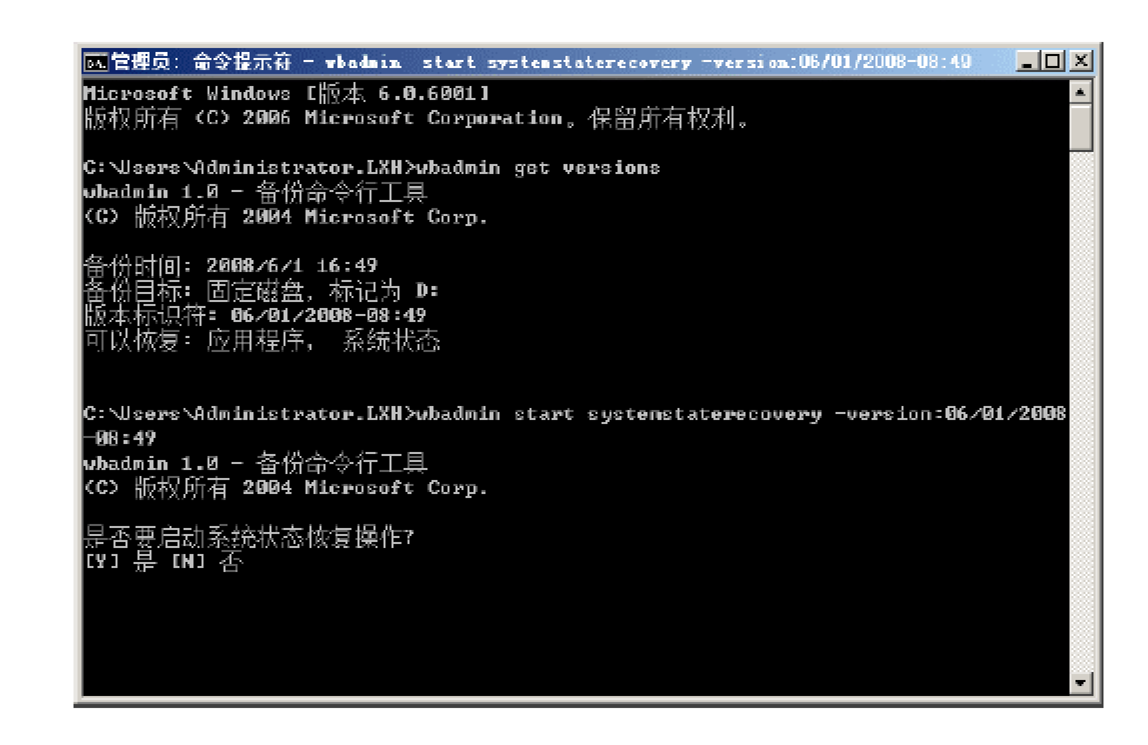


图 15-13 是否执行系统状态恢复

⑤ 输入“Y”(或“是”)并按 Enter 键，确认要执行系统状态恢复，提示网络管理员使用的复制引擎类型。如果复制引擎类型不同，系统状态将不能正确恢复，如图 15-14 所示。

⑥　恢复完成后，显示如图 15-15 所示的结果，提示用户需要重新启动计算机才能使恢复生效。需要注意的是，由于被恢复的系统文件比较多，重新启动服务器可能需要较长的时间。

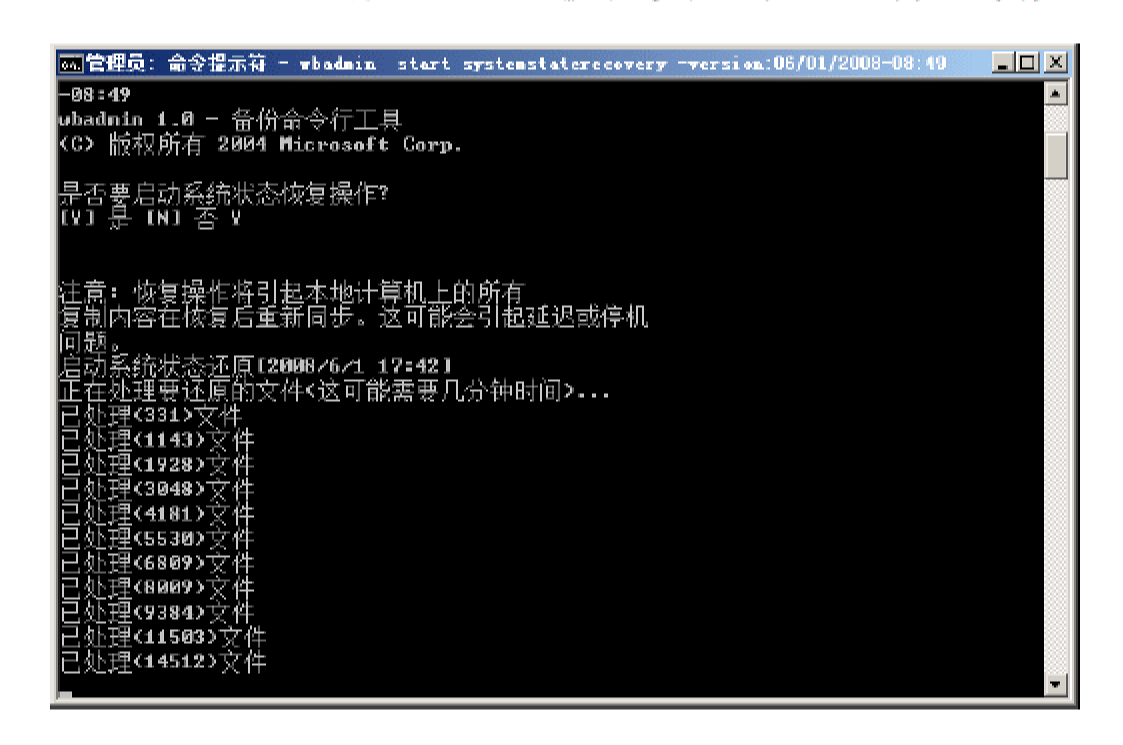


图 15-14　正在处理要还原的文件

图 15-15　恢复完毕

⑦　重新启动完成后，显示如图 15-16 所示的命令提示符窗口，提示系统状态已经成功恢复，按 Enter 键继续。

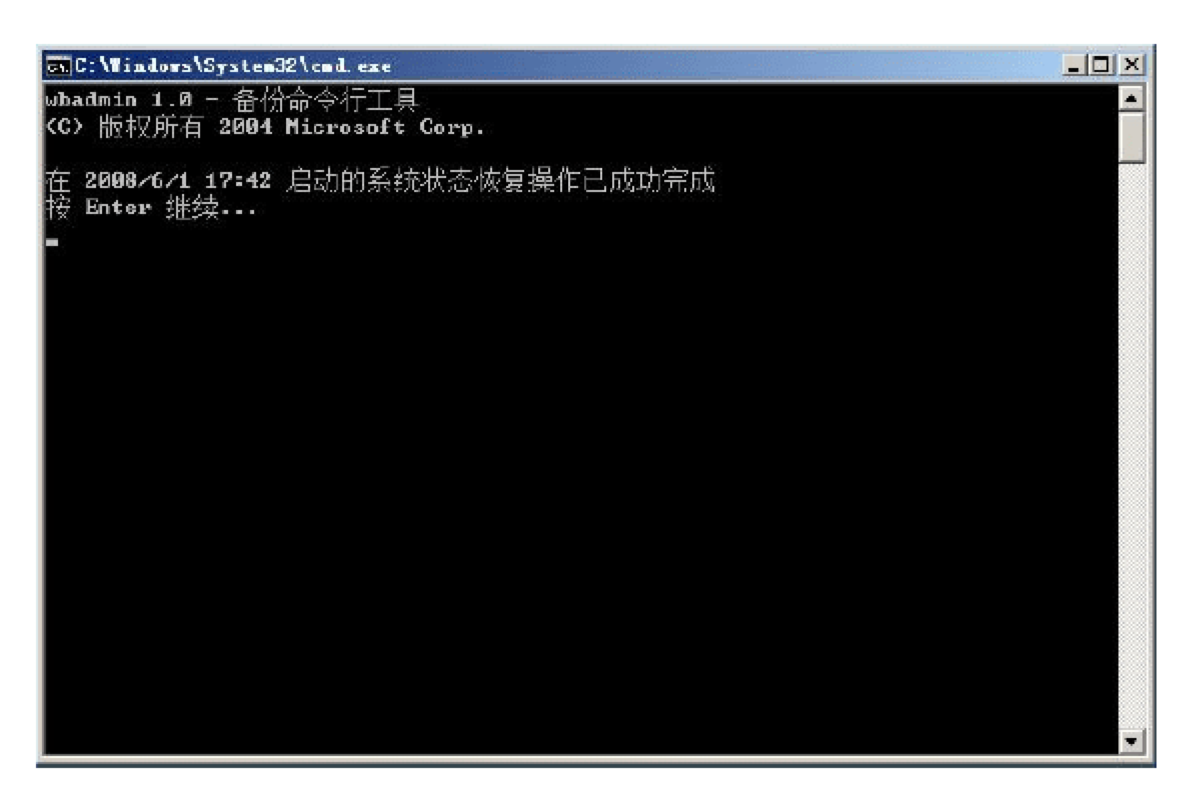


图 15-16　系统状态恢复成功

⑧　按 Enter 键即可进入系统。

15.1.3　恢复任意时间活动目录数据库备份

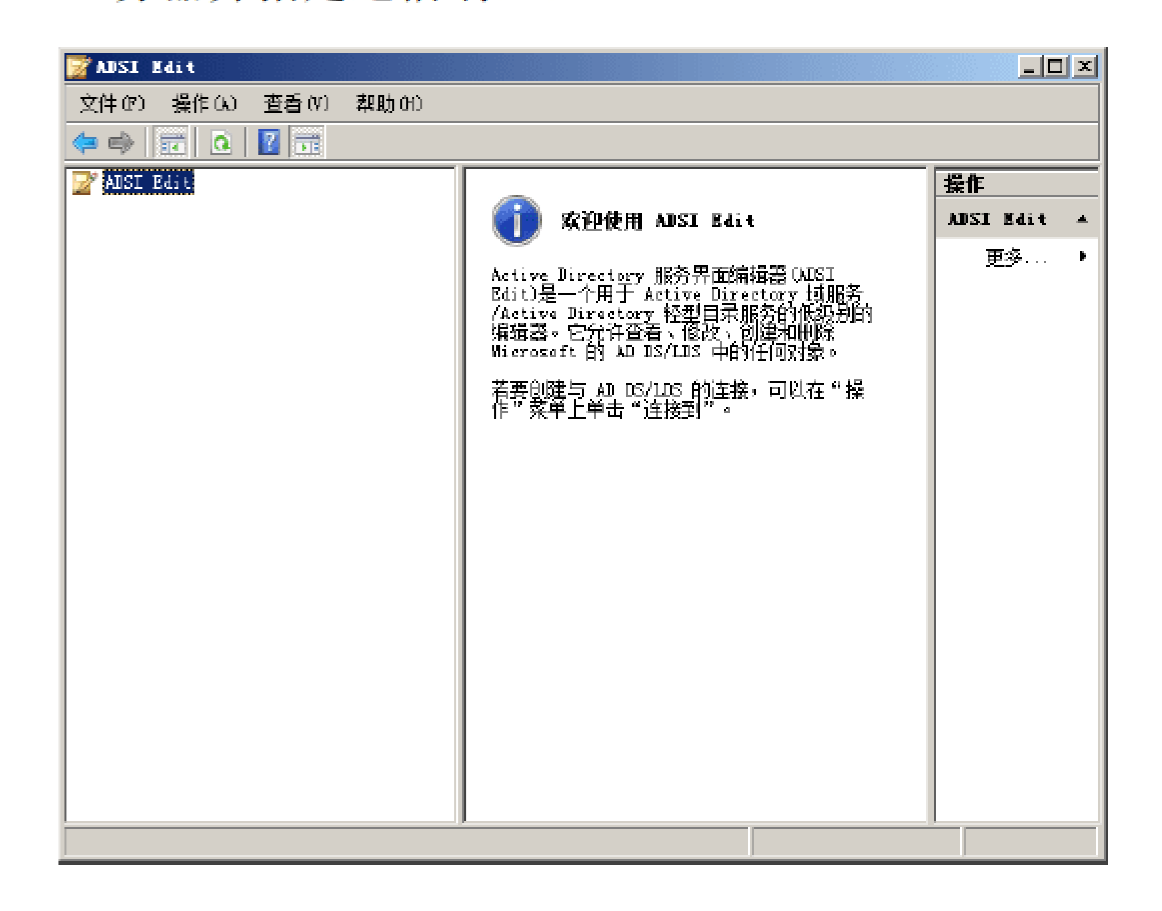
活动目录数据库的恢复需要一个良好的备份，即备份时间离当前时间不超过系统默认的时间限制。当活动目录中的一个对象被删除时，并不是彻底地消失。事实上，这时的对象变成了一个临时被标记为“墓碑”的记录。一定时间之后，系统才会将标记为“墓碑”的记录永久删除。因此，在“墓碑”记录被删除之前，管理员仍然可以通过数据库备份恢复被删除用户的账户信息。对于超过时间限制的备份，即使能够恢复，域中的客户端信息也将失去同步功能，彼此之间的安全通道将被破坏。



提示：在 Windows Server 2003 系统中“墓碑”记录的默认保留时间为 60 天，而在 Windows Server 2008 和 Windows Server 2003 SP1 系统中默认为 180 天。若想恢复任意时间的活动目录数据库备份，必须将“墓碑”记录保留足够长的时间。

① 单击“开始”→“运行”命令，在出现的“运行”对话框的“打开”文本框中，输入“adsiedit.msc”并按 Enter 键，显示如图 15-17 所示的 ADSI Edit 窗口。Active Directory 服务界面编辑器(ADSI 编辑)是一个轻型目录访问协议(LDAP)编辑器，类似于组策略编辑器和注册表编辑器，可用来管理 Active Directory 域服务中的对象和属性。

② 右击 ADSI Edit 并从弹出的快捷菜单中选择“连接到”命令，显示如图 15-18 所示的“连接设置”对话框。在“连接点”选项区域中，选择“选择一个已知命名上下文”单选按钮，并选择下拉列表中的“配置”选项。在“计算机”选项区域中，系统默认选择“默认(您登录到的域或服务器)”单选按钮，如果需要连接其他服务器，则可以选择“选择或键入域或服务器”单选按钮，选择服务器并指定通信端口。



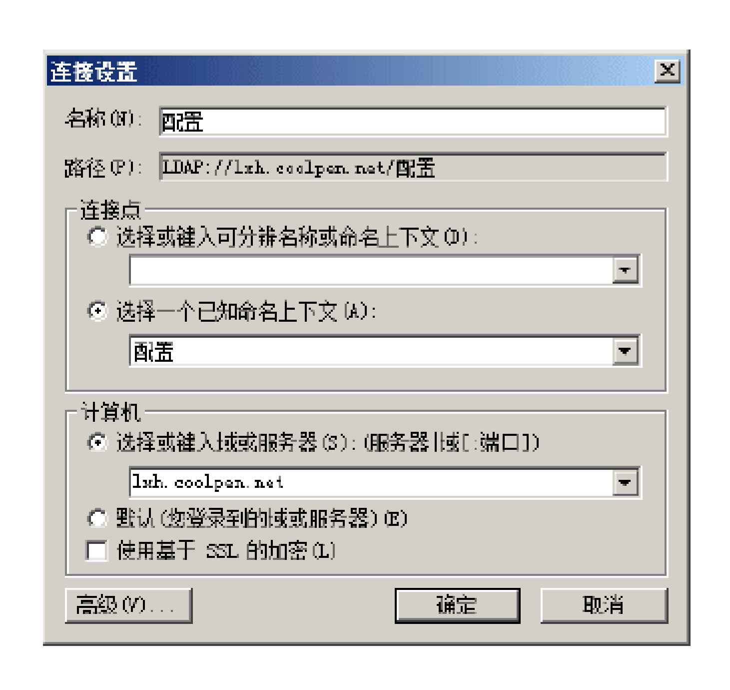


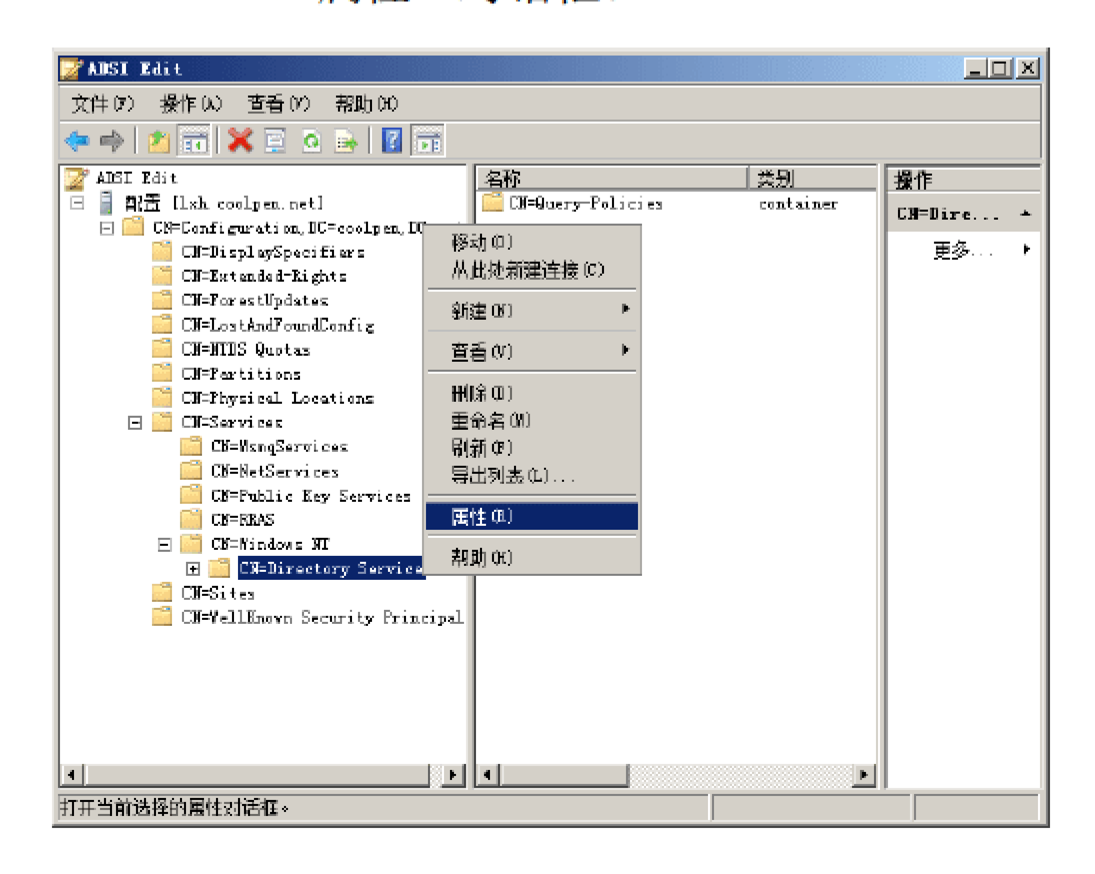


图 15-17　ADSI Edit 窗口

图 15-18　“连接设置”对话框

③ 单击“确定”按钮，返回 ADSI Edit 窗口，如图 15-19 所示。依次展开“配置[lxh.coolpen.net]”→ CN=Configuration,DC=coolpen,DC=net → CN=Services → CN=Windows NT → CN=Directory Service 节点。

④ 右击 CN=Directory Service，选择快捷菜单中的“属性”命令，显示如图 15-20 所示的“CN=Directory Service 属性”对话框。



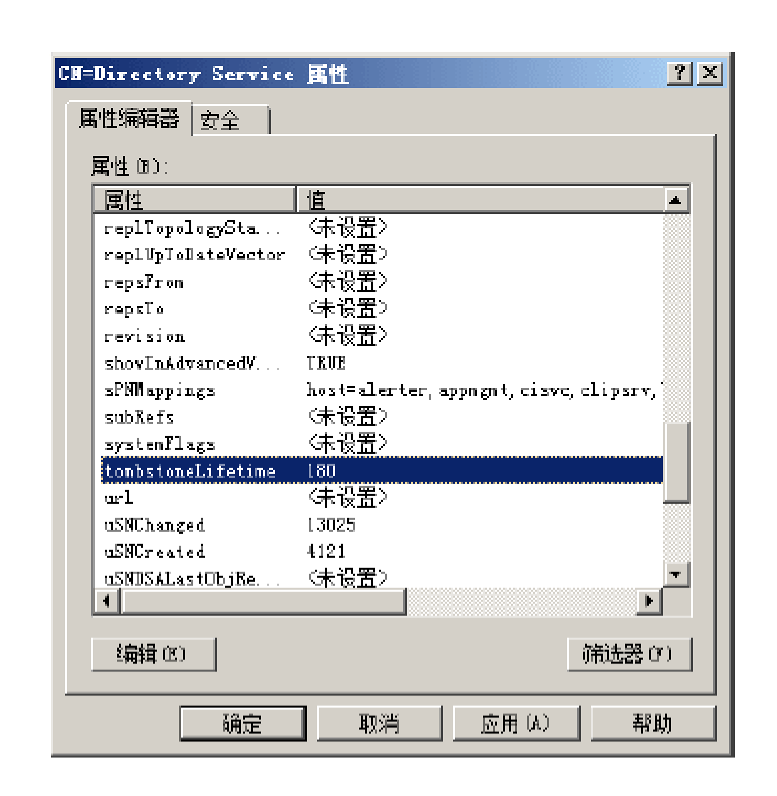


图 15-19　展开配置分区

图 15-20　“CN=Directory Service 属性”对话框

⑤ 选中 TombstoneLifetime 并单击“编辑”按钮，显示如图 15-21 所示的“整数属性编辑器”对话框。在“值”文本框中，输入新的“墓碑”生存时间即可，如 3600，默认时间单位为天。

⑥ 连续单击“确定”按钮保存设置，完成墓碑生存时间的修改。



图 15-21 “整数属性编辑器”对话框

15.1.4 使用授权还原模式恢复个别对象

在默认情况下，使用 Windows Server Backup 或 Ntbackup 还原 Active Directory 数据库的模式为非授权还原，使用此方式还原 Active Directory 后，将从其他的域控制器中同步复制数据库。同步完成后，系统管理员会发现已经删除的用户没有被正常恢复，因为此用户的“墓碑记录”已从其他服务器上被成功复制。此时，可以使用 Active Directory 备份恢复没有删除用户的数据库，然后使用“授权还原”的方法禁止域中的其他域控制器复制同步 Active Directory 数据库。主要操作步骤如下。

① 将需要还原的域控制器断开网络连接，并使用常规方法首先还原备份的 Active Directory 数据库。

② 单击“开始”→“运行”命令，在出现的“运行”对话框的“打开”文本框中，输入“cmd”并按 Enter 键，打开命令提示符窗口，输入如下命令：

```
ntdsutil
```

按 Enter 键运行，显示如图 15-22 所示的结果。

③ 在 ntdsutil 命令提示符后，输入如下命令激活 NTDS Active Directory 数据库实例：

```
activate instance ntds
```

按 Enter 键运行，显示如图 15-23 所示的结果。

图 15-22 启动 ntdsutil 管理工具

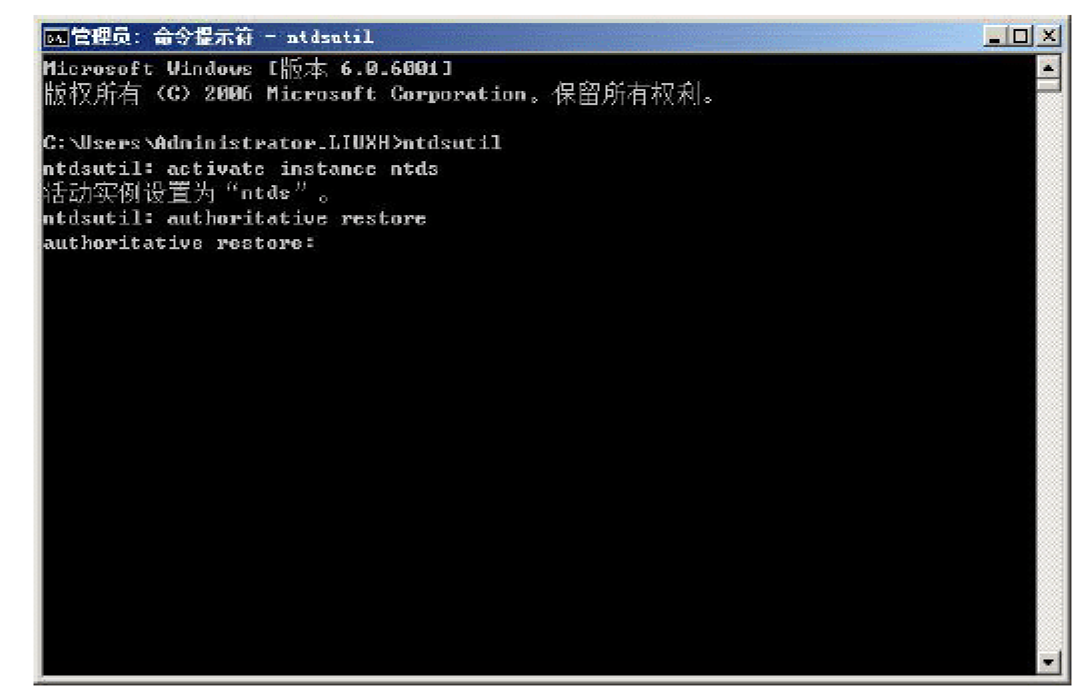


图 15-23 将 NTDS 设置为活动实例

④ 继续输入如下命令，将 NTDS 绑定到当前域控制器：

```
authoritative restore
```

按 Enter 键运行后转入 authoritative restore，继续输入如下命令：

```
restore object cn=lihn,ou=测试,dc=coolpen,dc=net
```

按 Enter 键运行，显示如图 15-24 所示的“授权还原确认对话”对话框。

⑤ 单击“是”按钮，开始执行恢复过程。执行结果如图 15-25 所示。

```
管理员: 命令提示符 - ntdsutil
Microsoft Windows [版本 6.0.6001]
版权所有 (C) 2006 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.LIUXH>ntdsutil
ntdsutil: activate instance ntds
活动实例设置为“ntds”。
ntdsutil: authoritative restore
authoritative restore:
authoritative restore:
authoritative restore:
authoritative restore: restore object cn=lihn,ou=测试,dc=coolpen,dc=net

授权还原确认对话
您确实想要执行这个授权还原?
是(Y)  否(N)
```

图 15-24 “授权还原确认对话”对话框

```
管理员: 命令提示符 - ntdsutil
authoritative restore: restore object cn=lihn,ou=测试,dc=coolpen,dc=net

正在打开 DIT 数据库... 完成现在时间是 05-31-08 10:33.17。
最近的数据库更新发生在 05-31-08 10:10.52。
增加属性版本号 100000。

计算需要更新的记录...
找到的记录: 0000000001
完成
找到 1 要更新的记录。

更新记录...
所剩记录: 0000000000
完成
成功的更新了 1 个记录。

已在当前工作目录中创建带有授权还原对象列表的下列文本文件:
        ar_20071220-222500_objects.txt
指定的对象均不具有此域中的返回链接。未创建任何链接还原文件。

Authoritative Restore 成功完成。

authoritative restore: _
```

图 15-25 开始恢复指定对象

⑥ 连续输入并运行两次 quit 命令，返回到命令窗口，完成已删除对象的恢复。



注意：在执行授权还原的过程中，要指明对象。

15.2 备份服务状态信息

Windows Server 2008 系统提供了大量的系统服务和应用服务，包括 DHCP 服务、DNS 服务、IIS 服务等，这些服务在企业的运营平台中发挥着关键的作用。通常情况下，服务器状态信息存储在注册表中，备份相应的键值即可实现对服务器状态信息的备份。当服务器角色出现故障或死机时，管理员只需使用服务状态信息备份，即可还原系统中正在运行的服务。

15.2.1 备份服务状态

① 以管理员账户登录系统，单击“开始”→“运行”命令，在出现的“运行”对话框的“打开”文

本框中输入“regedit”命令并按 Enter 键，打开“注册表编辑器”窗口。

② 依次展开 HKEY_LOCAL_MACHINE→SYSTEM→CurrentControlSet→Services 节点，各个服务的状态都存储在下面的子项中，网络管理员只要将其备份出来即可，如图 15-26 所示。

③ 右击 Services 并选择快捷菜单中的“导出”命令，显示“导出注册表文件”对话框，选择备份文件所要存储的路径，并指定备份的文件名，单击“保存”按钮即可完成 Windows 服务状态的备份。备份的文件是扩展名为.reg 的注册表文件，如图 15-27 所示。

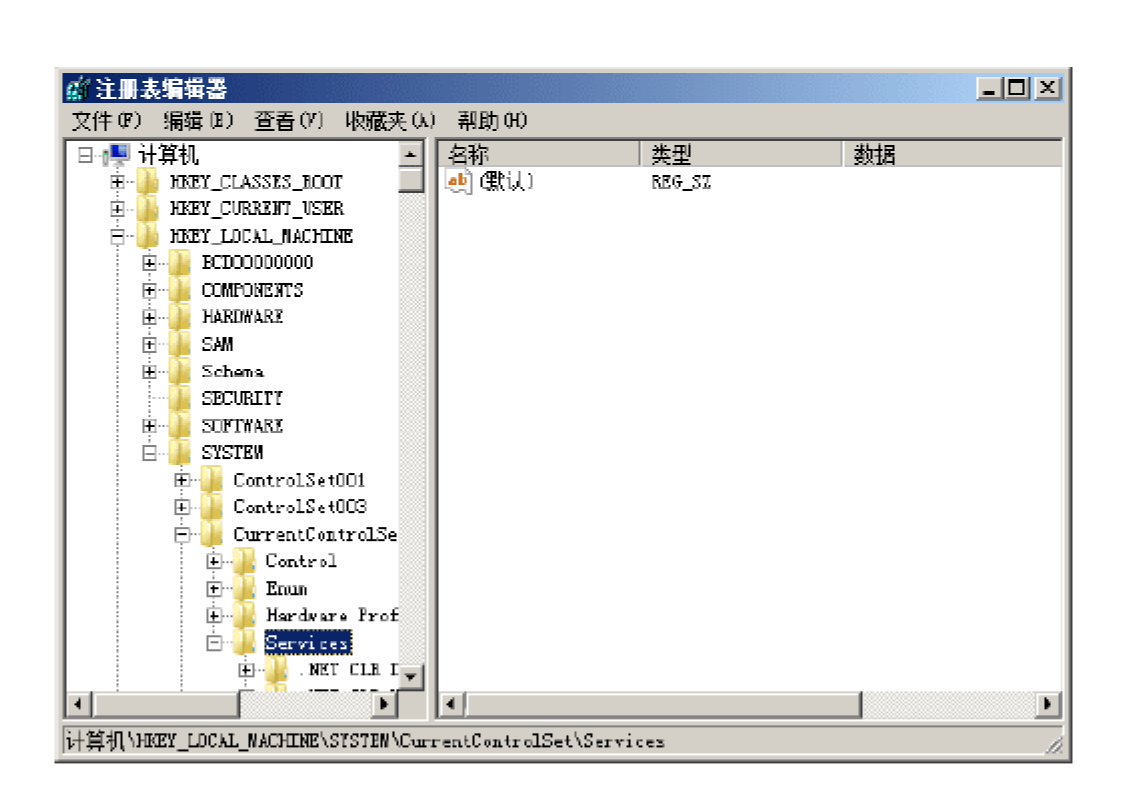


图 15-26　服务信息在注册表中的位置

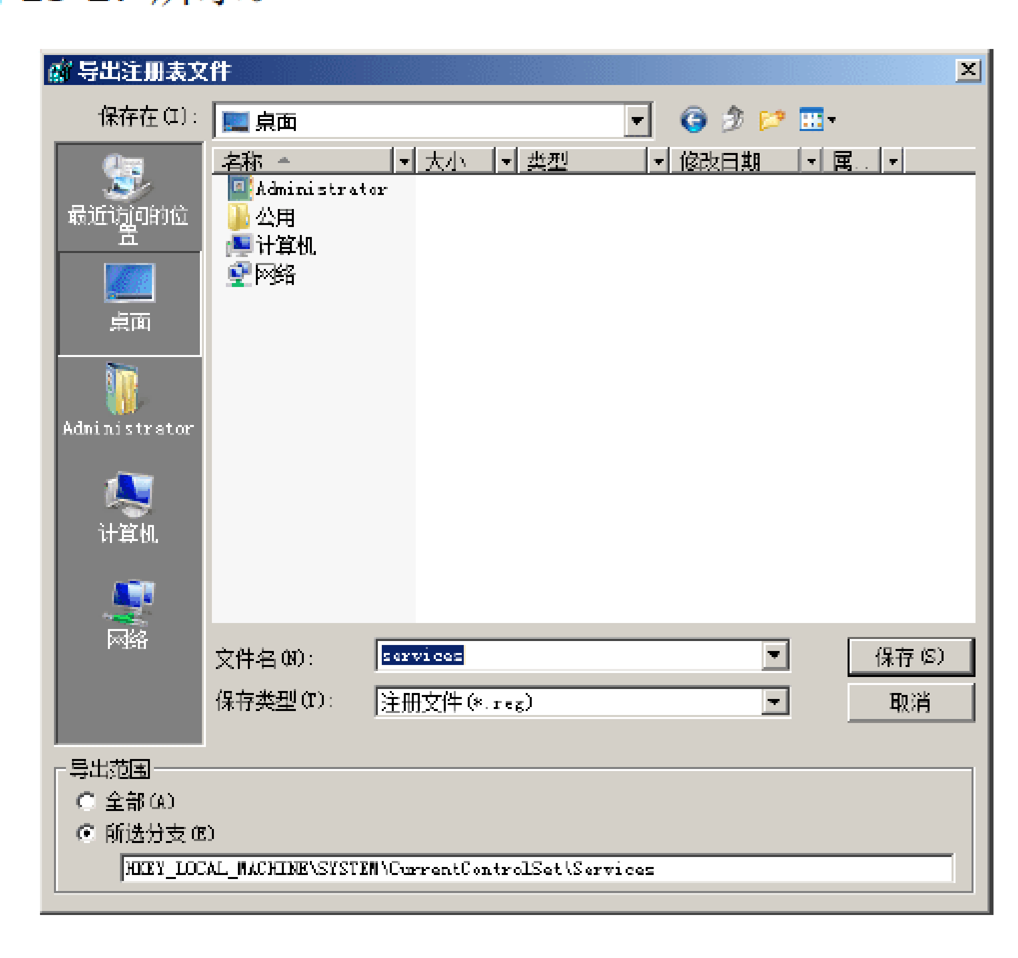


图 15-27　“导出注册表文件”对话框

15.2.2　恢复服务状态

当 Windows 服务出现问题的时候，只要选择导出的注册表文件，双击运行，将备份的文件重新导入到注册表中，即可解决系统服务出现的问题，如图 15-28 所示。成功导入注册表文件后，需要重新启动计算机才能使服务生效。

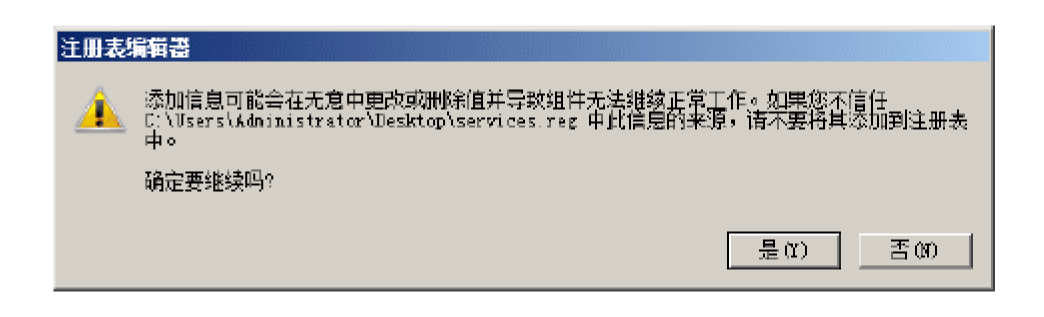


图 15-28　导入注册表文件

15.3　DHCP 服务器备份

在规模较大的局域网中，网管一般会采用 DHCP 服务器为客户机统一分配 TCP/IP 配置信息。但如果因为管理员的误操作或其他一些因素，使 DHCP 服务器的配置信息出错或丢失，将会直接导致网络内的计算机不能正常访问网络。如果采用手动恢复非常麻烦，而且工作量较大。同时，在 DHCP 服务器中还可能包含多个作用域，并且每个作用域中又会包含不同的 IP 地址段、网关地址、DNS 服务器等参数。因此，对 DHCP 服务器的备份工作，也是这些网络服务器中一项不可缺少的工作。

15.3.1　内置工具

1. 备份 DHCP 数据库

在 DHCP 服务器中，已经内置了备份和还原功能，而且操作也非常简单。

① 在 DHCP 控制台窗口中，右击 DHCP 服务器名选项，从弹出的快捷菜单中选择“备份”命令，如图 15-29 所示。

② 在打开的“浏览文件夹”对话框中，指定备份文件的存放路径，单击“确定”按钮，即可完成 DHCP 服务器配置信息的备份工作，如图 15-30 所示。

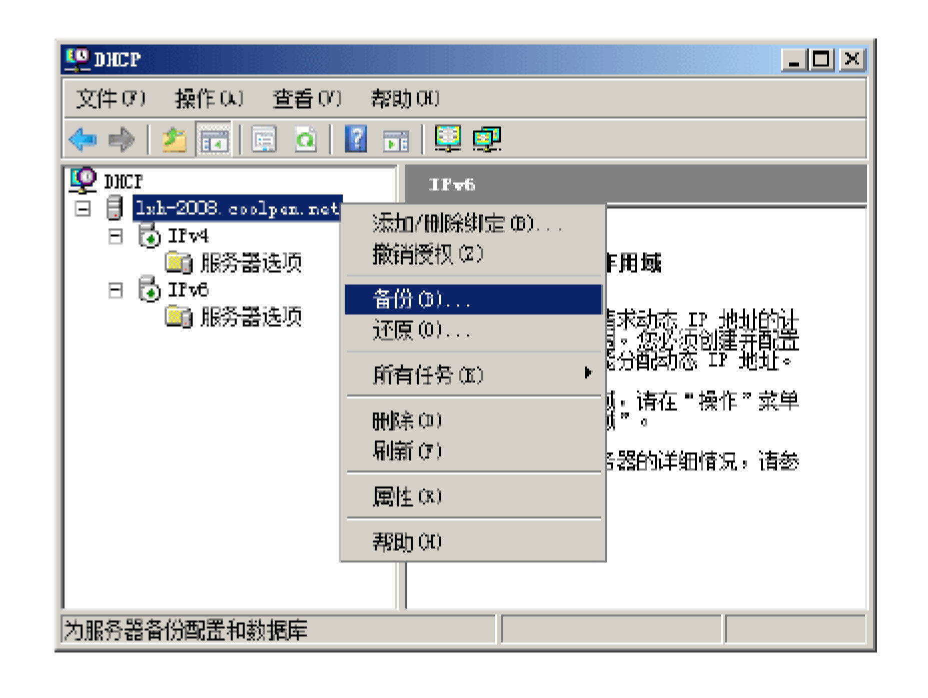


图 15-29　DHCP 控制台

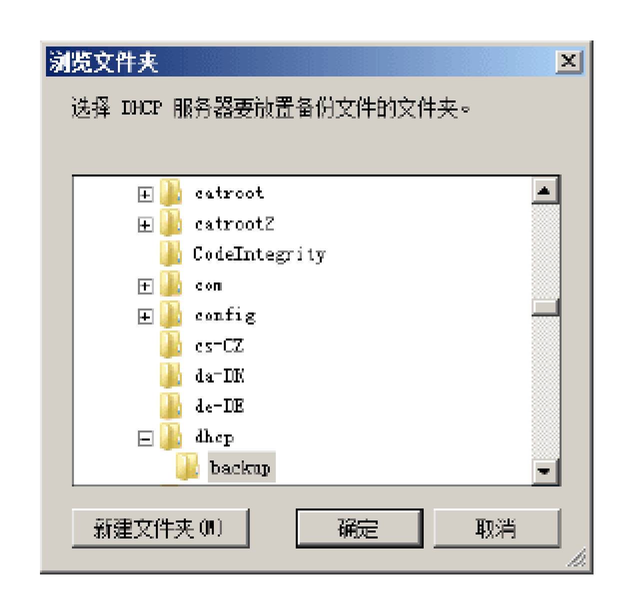


图 15-30　存放 DHCP 备份文件的位置

2. 还原 DHCP 数据库

① 如果 DHCP 配置信息损坏，需要进行恢复时，可右击 DHCP 服务器名选项，从弹出的快捷菜单中选择“还原”命令，如图 15-31 所示。

② 系统显示“浏览文件夹”对话框，用户可以根据备份文件的路径来指定备份文件所在的路径，如图 15-32 所示。

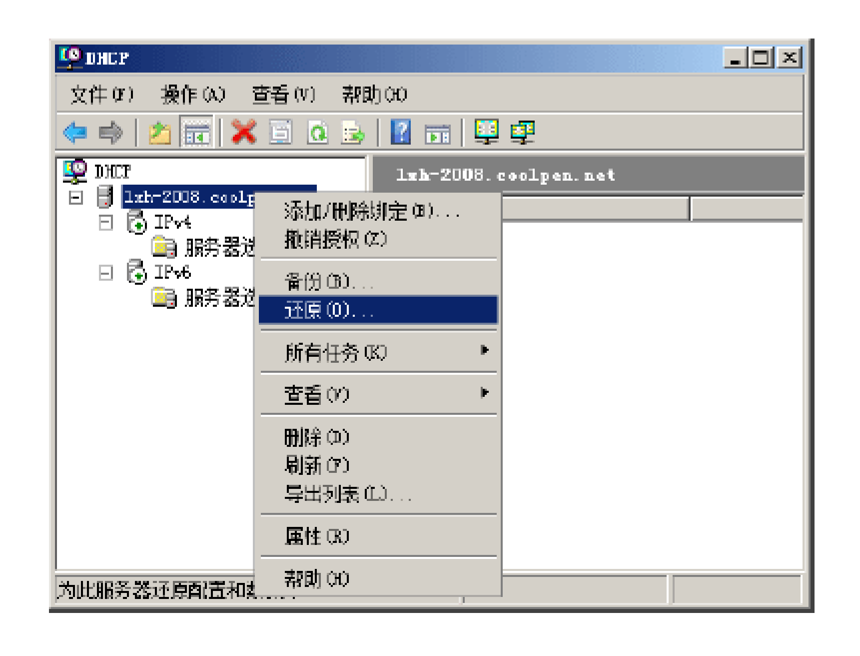


图 15-31　还原 DHCP 数据库



图 15-32　指定备份文件的位置

③ 单击“确定”按钮后，显示 DHCP 信息提示框，如图 15-33 所示。为了使改动生效，必须停止 DHCP 服务并重新启动该服务。



图 15-33　DHCP 提示信息

15.3.2 NETSH 命令

除上述方式外，管理员还可以通过命令行的方式进行备份操作，从而达到备份 DHCP 服务数据库的目的。

1. 备份 DHCP 数据库

以管理员账户登录服务器系统，在“命令提示符”窗口中，输入以下命令：

```
netsh dhcp server export c:\dhcp.txt all
```

按 Enter 键确认，即可完成对 DHCP 服务器的备份，所有的 DHCP 信息将被存储在文本文件中，如图 15-34 所示。

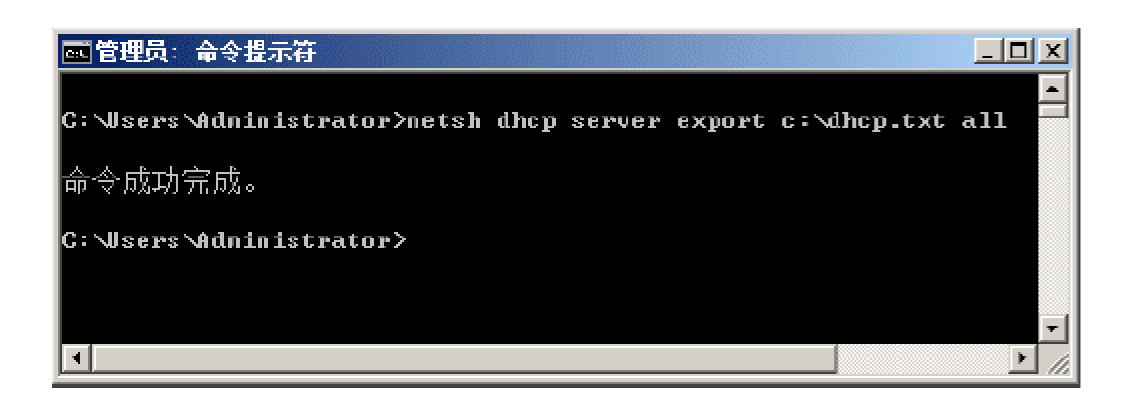


图 15-34　脚本方式备份 DHCP 服务数据库

2. 还原 DHCP 数据库

如果需要还原 DHCP 数据库，只需在“命令提示符”窗口中，输入以下命令：

```
netsh dhcp server import c:\dhcp.txt all
```

按 Enter 键确认，即可完成 DHCP 服务器数据库的恢复。

15.3.3 DHCP 移植

如果要将一台 Windows Server 2008 系统的 DHCP 服务器中的数据库，移植到另一台 Windows Server 2008 系统的 DHCP 服务器中，同样使用 netsh 命令可以轻松地完成。

① 在源 DHCP 服务器中，进入“命令提示符”窗口，运行 netsh dhcp server export c:\dhcp.txt all 命令，将 DHCP 服务器中的数据库备份到 C 盘的 dhcp.txt 文件中。

② 将 dhcp.txt 备份文件复制到目标 DHCP 服务器的 C 盘根目录下，在“命令提示符”窗口中，运行 netsh dhcp server import c:\dhcp.txt all 命令，即可完成 DHCP 服务器数据库的移植工作。

移植 DHCP 服务器时，应注意如下事项。

- 在备份数据库文件夹时，必须选择服务器的一个本地驱动器。
- DHCP 服务会在正常操作的过程中，自动创建 DHCP 数据库的备份文件。该数据库备份副本默认的存储位置为 systemroot\System32\Dhcp\Backup。
- 建议用户使用 Windows 备份程序(ntbackup.exe)，或非 Microsoft 备份软件将 DHCP 数据库备份到本地驱动器以外的位置。
- 如果将手动创建的 DHCP 数据库备份，存储在与 DHCP 服务器每 60min 创建一次的同步备份相同

的位置，则进行自动备份时，手动备份将被覆盖。

15.4　磁盘配额备份

使用 Windows 系统提供的磁盘配额功能，可以对每个用户所使用的磁盘容量进行限制。但是如果服务器由于某些原因，或者因为重新安装服务器操作系统和其他原因造成配置信息丢失，那么手工恢复起来就需要大量的时间。因此网络管理员在备份系统服务的同时，还应备份好磁盘配额项目的信息。

15.4.1　备份磁盘配额

① 右击启用磁盘配额的分区(以 D 盘为例)，选择快捷菜单中的“属性”命令，在显示的对话框中切换到“配额”选项卡，单击“配额项”按钮，显示如图 15-35 所示的“(D:)的配额项”窗口。

② 右击希望备份的配额项目，并选择快捷菜单中的“导出”命令，显示“导出配额设置”对话框。指定保存备份文件的目录后单击“确定”按钮，即可开始备份。也可以同时导出多个配额项目。



图 15-35　“(D:)的配额项”窗口

15.4.2　还原磁盘配额

在配额项目管理对话框中，单击“配额”→“导入”命令，即可选择已保存的备份文件。还原磁盘配额设置时，系统会显示如图 15-36 所示的“磁盘配额”对话框。单击“是”按钮，即可完成磁盘配额项目的还原。

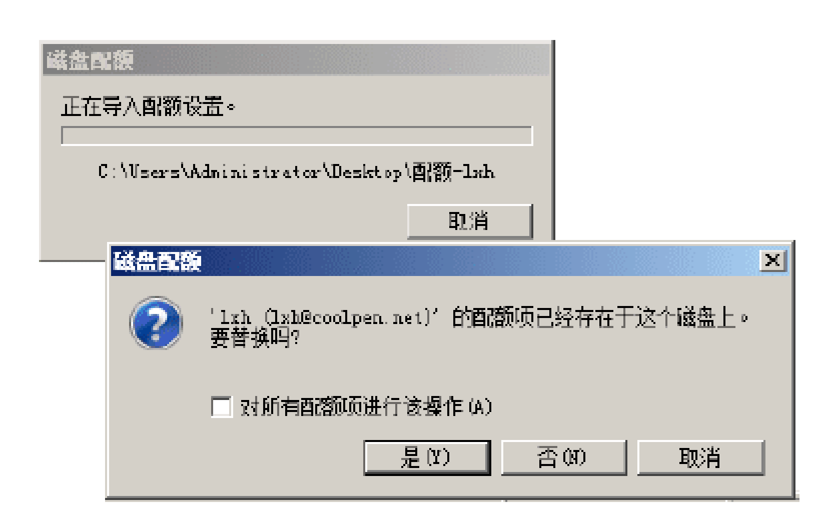


图 15-36　“磁盘配额”对话框

15.5　DNS 服务器备份

DNS 服务器担负着域名解析的工作，其重要性不言而喻。如果网络中的 DNS 服务器出现问题或者信息数据丢失的话，则服务器将无法完成域名的解析工作。因此，平时要经常对 DNS 服务器的数据信息进行备份。当发现 DNS 服务器出现问题时，可以方便地使用备份文件快速恢复 DNS 服务器的工作。DNS 服务器数据的备份分两步进行：首先，要备份注册表中的 DNS 服务器的相关信息；其次，要备份域名解析时所使用的 DNS 数据信息。

15.5.1　DNS 注册表信息备份

1. 备份 DNS 服务信息

① 打开注册表编辑器，在左侧的层次列表中依次展开 HKEY_LOCAL_MACHINE→System→CurrentControlSet→Services→DNS”节点，只要将此键值下的所有数据备份出来即可。

② 选中 DNS 项目，单击“文件”菜单中的“导出”命令，显示“导出注册表文件”对话框，指定备份文件的存放路径和文件名即可，如图 15-37 所示。

> **注意：在备份服务状态的时候，其实就已经备份了 DNS 信息，但是为了备份和还原 DNS 数据的简易性和方便性，建议对 DNS 数据进行单独备份。**

2. 备份 DNS Server 服务信息

① 打开注册表编辑器，在左侧的层次列表中依次展开 HKEY_LOCAL_MACHINE→Software→Microsoft→Windows NT→CurrentVersion→DNS Server 节点，将此键值下的所有数据备份出来即可。

② 选中 DNS Server 项目，单击“文件”菜单中的“导出”命令，显示“导出注册表文件”对话框，指定备份文件的存放路径和文件名称即可完成数据的保存，如图 15-38 所示。

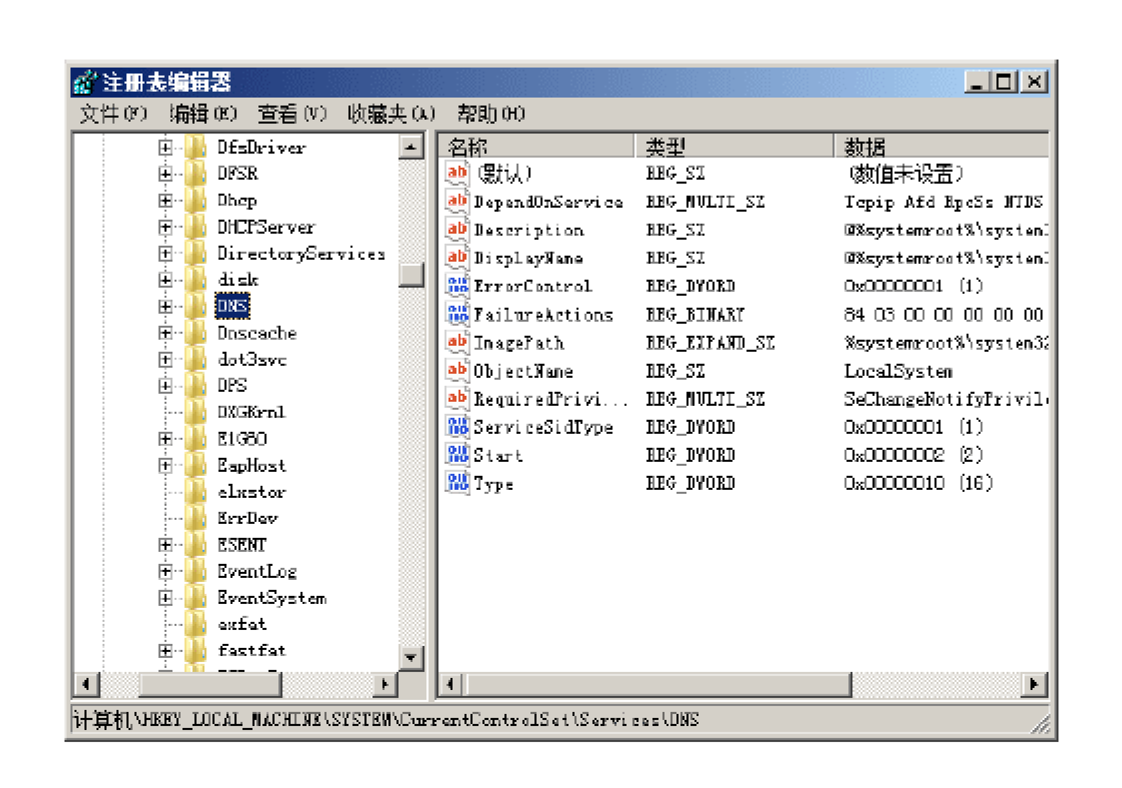


图 15-37　备份注册表的 DNS 服务信息

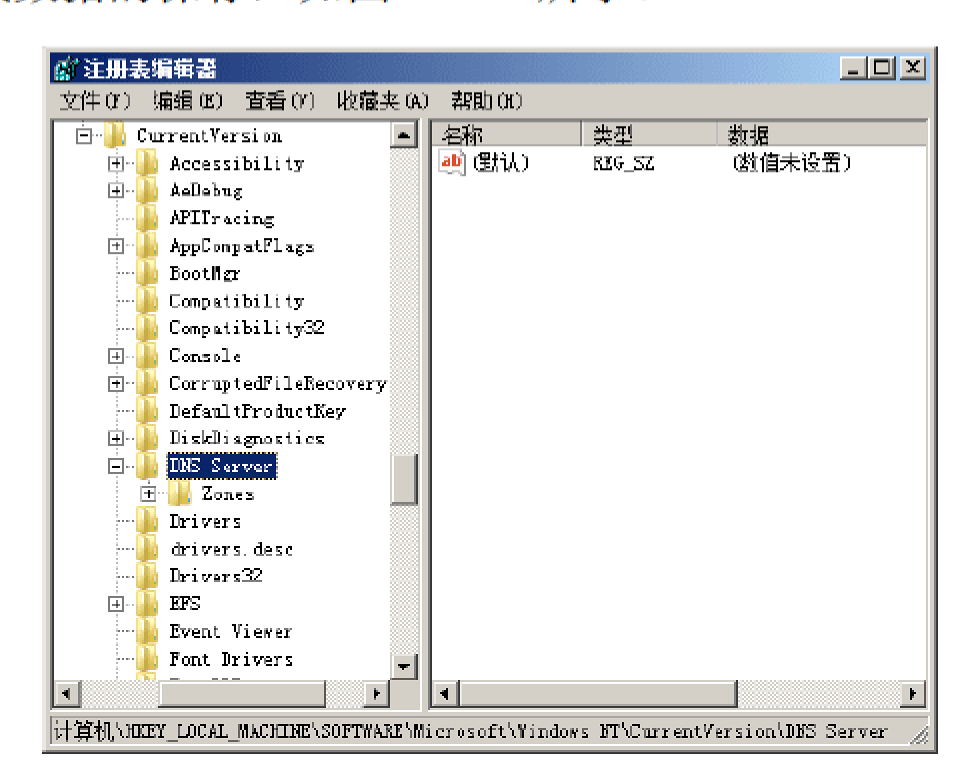


图 15-38　备份注册表的 DNS Server 服务信息

15.5.2　DNS 数据文件备份

“DNS 注册表信息备份”备份的是注册表中的信息，但其中并不包含域名解析时，所使用的域名数据信息，这部分内容需要单独进行备份。

打开 DNS 服务器的资源管理器，进入到 c:\windows\system32\dns 目录，将后缀为.dns 的所有文件备份出来，这些文件中存储的就是域名解析时所使用的域名数据信息，这样就完成了域名数据的备份操作，如图 15-39 所示。

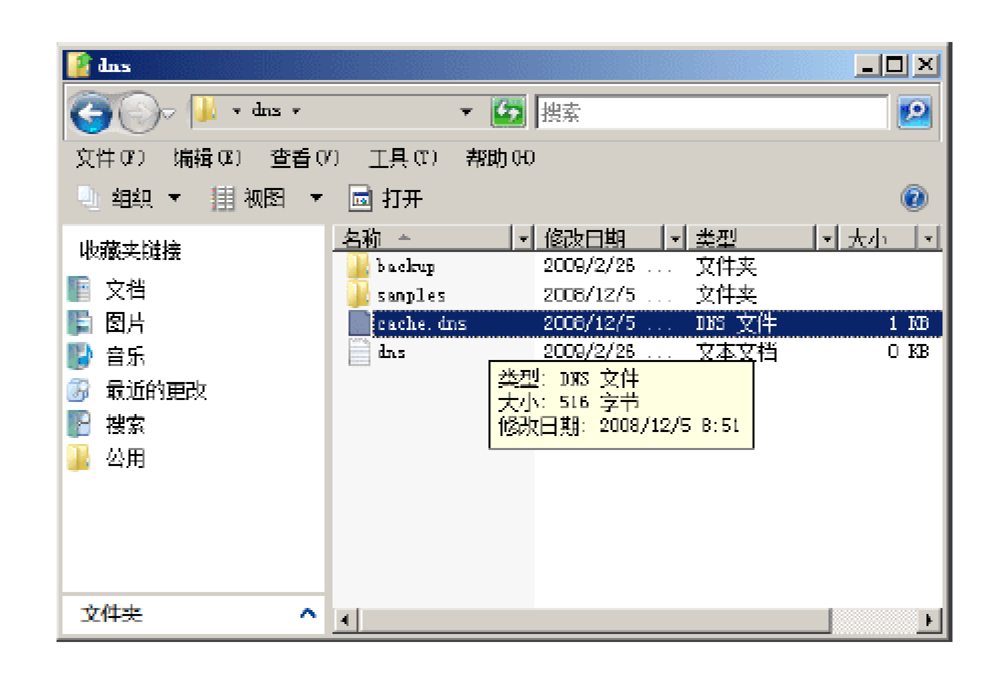


图 15-39　备份 DNS 数据文件

15.5.3 DNS 数据还原

当 DNS 服务器出现问题，就可以使用备份的两部分数据进行恢复。

① 运行备份的两个注册表文件，将其导入到注册表中。

② 将后缀为.dns 的所有文件覆盖 c:\windows\system32\dns 目录下所有的同名文件，即可完成 DNS 服务器的数据恢复。



注意：在完成还原 DNS 服务器的工作后，建议重新启动 DNS 服务器。

15.6 WINS 服务器备份

WINS 服务器为 NetBIOS 名称提供名称注册、更新、释放和转换等服务，这些服务允许 WINS 服务器维护一个将 NetBIOS 名链接到 IP 地址的动态数据库，大大减轻了网络的负担。在默认情况下，网络上的每一台计算机的 NetBIOS 名称，都是通过广播的方式来进行更新的。如果网络规模比较大，“广播”无疑会加重网络的负担。因此，对大中型网络而言，备份 WINS 服务器是非常重要的。

15.6.1 备份 Wins 数据库

① 打开 WINS 控制台窗口。右击 WINS 服务器，并从弹出的快捷菜单中选项“备份数据库”命令，如图 15-40 所示。

② 系统显示“浏览文件夹”对话框。选择 WINS 数据备份的位置，单击“确定”按钮。备份过程完成之后，显示如图 15-41 所示的 WINS 提示框。单击“确定”按钮，即可完成 WINS 数据库的备份。

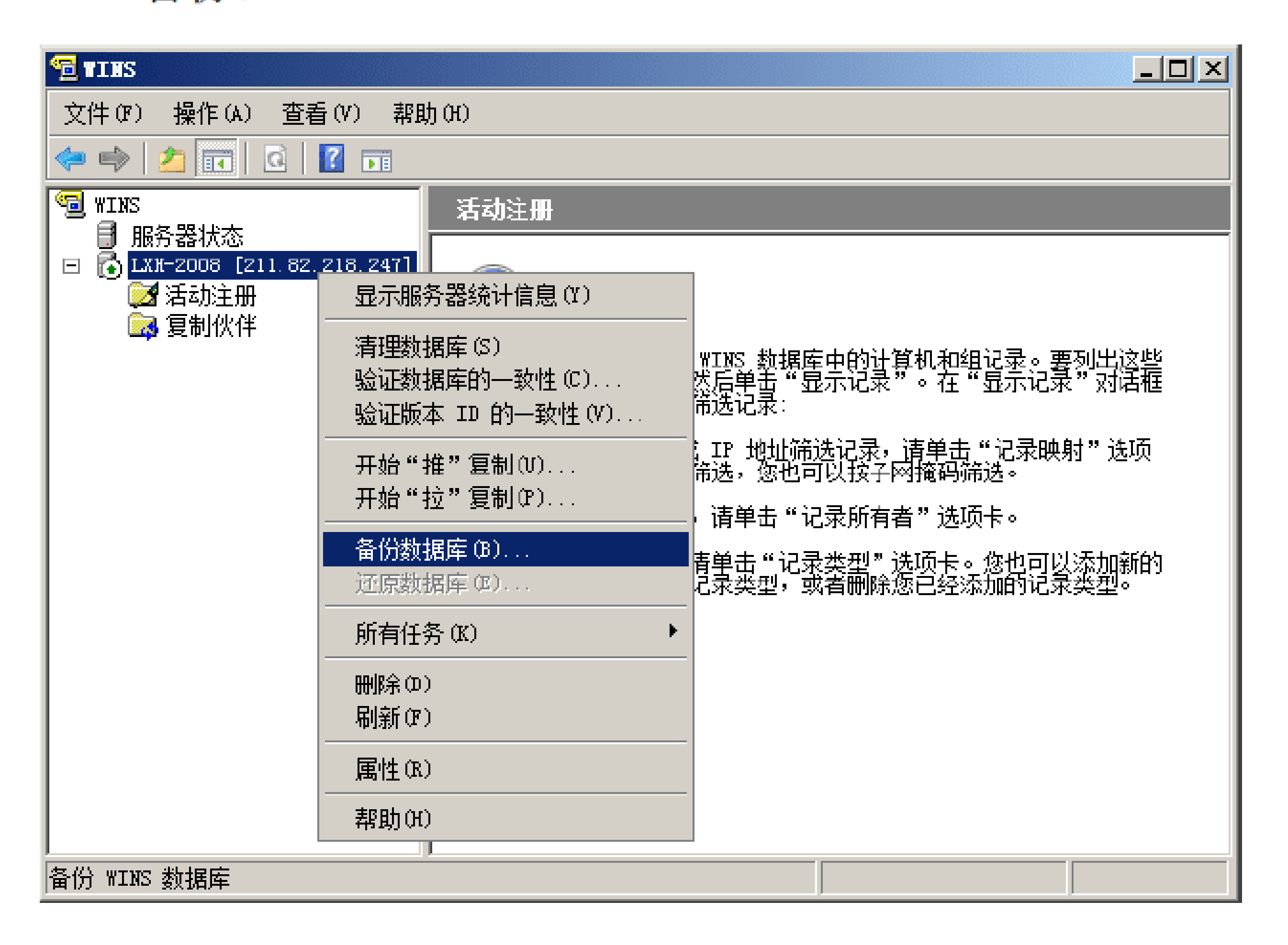


图 15-40 备份 WINS 服务数据库



图 15-41 数据库备份完成提示

15.6.2　还原 Wins 数据库

① 右击控制台中所使用的 WINS 服务器，从弹出的快捷菜单中选择“还原数据库”命令，系统会显示“浏览文件夹”对话框。

② 选择 WINS 数据库还原的位置，单击“确定”按钮开始还原。还原过程完成之后，重新启动 WINS 服务即可完成 WINS 服务器的还原工作。

15.7　网络配置备份

作为一名网络管理员，首先要维护网络安全、正常地运行，在网络发生故障时能迅速进行恢复。在网络故障恢复过程中，尤为重要的是服务器网络设置的恢复。Netsh 是 Windows 2000/XP/2003/Vista/2008 操作系统自身提供的命令行脚本实用工具，允许用户在本地或远程显示和修改当前正在运行的计算机的网络配置，另外也可以将配置脚本保存在文本文件中。

15.7.1　备份服务器的网络设置

常规服务器的网络设置包括 IP 地址设置、接口、端口代理、远程访问、路由、DNS 代理、NAT、DHCP 中继代理配置等。这些网络参数的设置，根据服务器在网络中所起的特殊作用而有所不同。只有对网络服务器的设置进行了相应的备份，才能在网络设置遇到毁灭性破坏时，迅速并且及时地恢复网络。

在命令行模式下输入如下命令：

```
netsh dump >d:\NFC-lxh-2008.txt
```

按 Enter 键确认，命令行成功执行，将网络设置备份到 c:\bak1txt 文件中，该文件为一个文本文件，如图 15-42 所示。

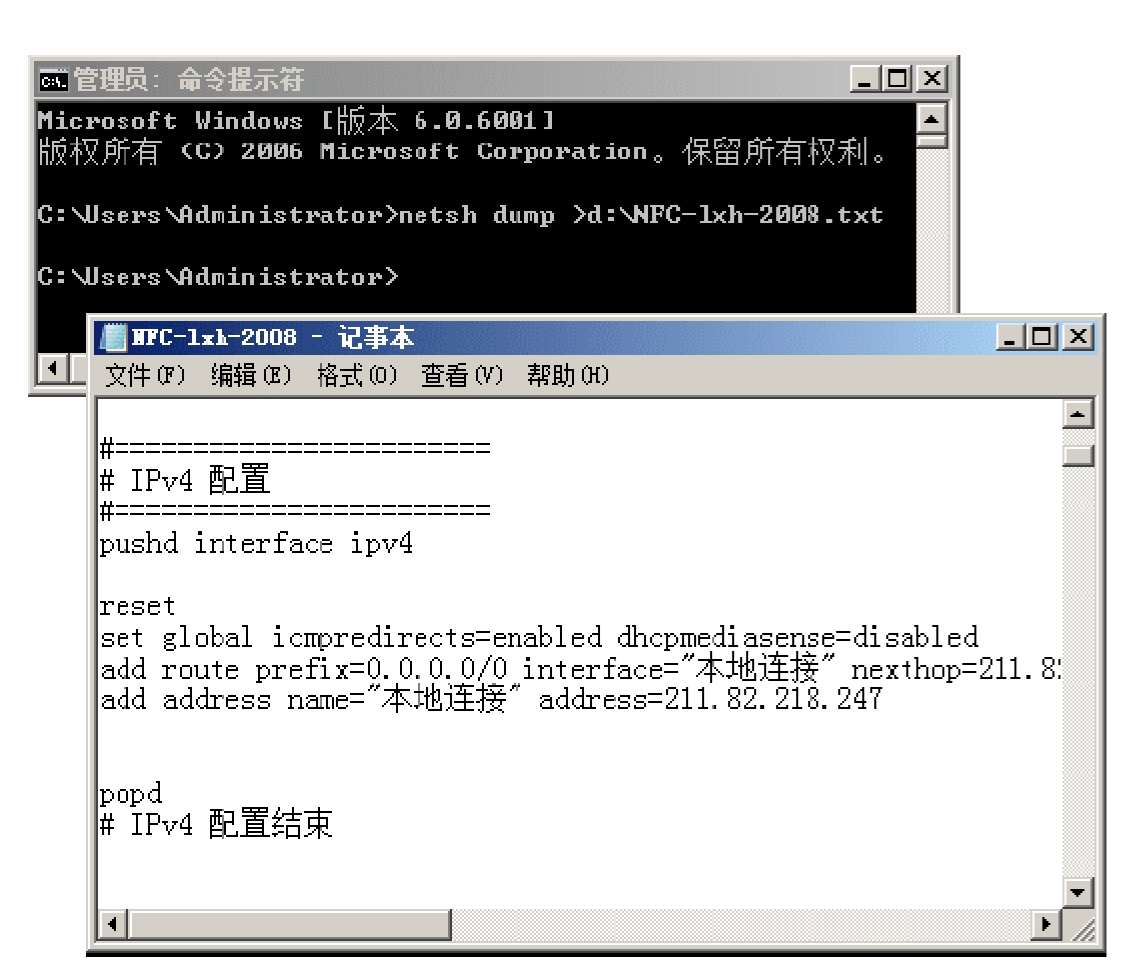


图 15-42　备份服务器的网络设置

15.7.2　恢复服务器的网络设置

在进行网络设置调整时，如果发生了操作失误，或者服务器的网络发生故障，可以利用备份快速恢复网络设置。

在命令行模式下输入如下命令：

```
nesh exec d:\NFC-lxh-2008.txt
```

按 Enter 键确认，命令成功执行，即可将已经备份好的网络设置还原到系统中。该命令非常适合网络管理人员用来对服务器网络设置进行备份和恢复管理。